THE THREE LINES OF DEFENSE – WHAT ARE THE RESULTS?

GRANT HARBRECHT
FIFTH THIRD BANK, CHIEF COMPLIANCE OFFICER
MAY 24, 2017

FIDUCIARY & INVESTMENT RISK MANAGEMENT ASSOCIATION (FIRMA)
31ST NATIONAL RISK MANAGEMENT TRAINING CONFERENCE

Agenda

- Welcome and Introduction
- Foundational: What are the Three Lines of Defense?
- Regulatory Requirements and Industry Expectations
- Industry "Best Practices" and/or Improvements
- Where have the lines been drawn?
- Where do we go from here?
- Closing Comments

Foundational: What are the Three Lines of Defense?

- **First Line**
  - Front line units, business units or functions that create risk (i.e., the "line of business") = primary risk takers
  - <u>But</u> note the development and growing role of control functions within the First Line (1.5) versus the actual business process owners (1.0)
- **Second Line**
  - Independent risk management functions = i.e., independent of the lines of business (e.g., Credit Risk, Market Risk, Compliance, Operational Risk, etc.)
- **Third Line**
  - Internal audit = accountable to the Board

Regulatory Requirements and Industry Expectations

- **Office of the Comptroller of the Currency (OCC)**
  - OCC Bulletin 2016-25: issued July 29, 2016 → Corporate and Risk Governance booklet of the Comptroller's Handbook
  - "Heightened Standards": specific criteria for OCC "covered banks" [12 CFR 30, Appendix D]; a "covered bank" is, generally speaking, those with average total consolidated assets of $50 billion or greater
  - "Fiduciary Activities of National Banks" [12 CFR 9] – for more information on a national bank's fiduciary responsibilities and compliance

- **Federal Reserve Board (FRB)**
  - "Compliance Risk Management Programs and Oversight at Large Banking Organizations with Complex Compliance Profiles [SR 08-08 / CA 08-11, issued October 16, 2008]
  - Expansion of SR 08-08 to cover conduct risk programs? FRB to issue separate guidance on conduct risk management?

Industry "Best Practices" and/or Improvements

Is there Consistency? Must there be?

- **Industry "best practice"**
  - No single risk management structure works for all banks
  - The sophistication and formality of structures and practices should be proportionate to the size and complexity of the subject bank
    - Factors may include scope and complexity of operations, types and size of assets (e.g., global vs. regional banks vs. community banks; primarily domestic banking model vs. international banking; sales & trading vs. fiduciary vs. retail banking; etc.)

- **Improvements**
  - More process and more resources focused on understanding underlying <u>root causes</u> of control issues versus treating just the symptoms → results in better longer term solutions
    - But significant regulatory and management pressure to get control issues fixed as quickly as possible
  - Monitoring and testing, and continued efforts to rationalize who tests what → emergence of robotics as a common discussion topic regarding ways to improve efficiency

Industry "Best Practices" and/or Improvements

Is there Consistency? Must there be?

- **Improvements (continued)**
  - Regulatory change management governance processes
  - Self-identification of control issues: specific targets vs. other methods
    - Working to demonstrate a culture of proactive self-management
  - Governance routines and reporting
    - Active line of business management participation and engagement in Compliance and Operational Risk routines
    - Better reporting of risks, underlying causes and points of accountability (e.g., looking to business leaders vs. compliance leaders to know the issues)
    - Overall heightened awareness and deeper understanding of the issues and risks

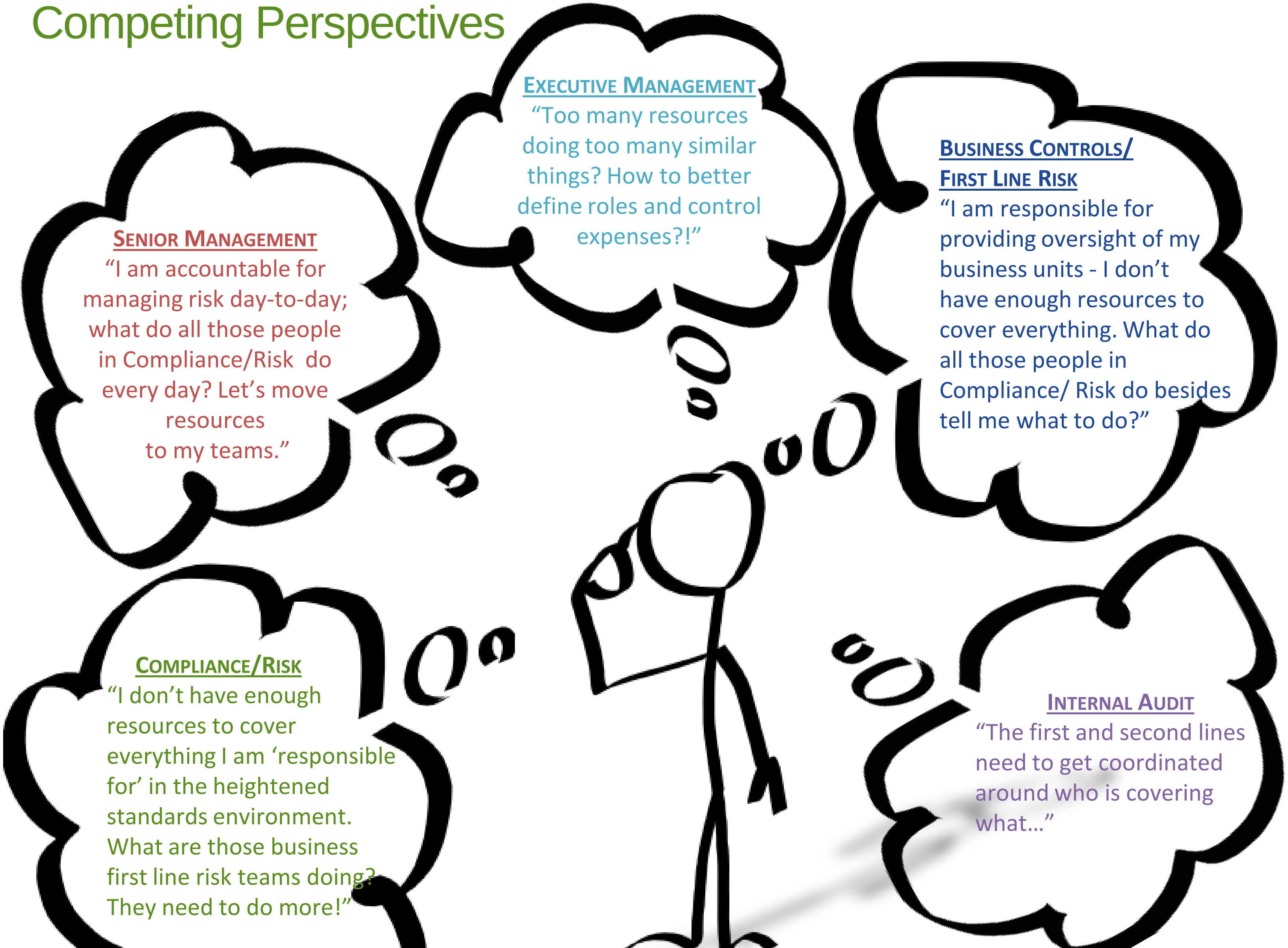
Where have the lines been drawn?

The Challenge

- As a result of the global financial crisis, the “risk” pendulum swung toward greater numbers of independent risk resources <u>and</u> increasing accountability of front line units that create risk.
    - Is the pendulum swinging back as more controls and quality assurance functions have been added to the financial services industry and embedded into first line activities?
- Generally, OCC and FRB have been examining to a three lines of defense model, although variability in guidance/implementation exists.
- Financial institutions of all sizes struggle to balance the need to demonstrate proactive risk management across the enterprise with investor/industry demands to operate as efficiently as possible.

Where have the lines been drawn?

Competing Perspectives



ENTERPRISE RISK MANAGEMENT
→ EFFECTIVE & EFFICIENT

Where do we go from here?

- **How to do more with less?**
  - Accelerate technology enablement and adoption of machine learning and robotic processes to improve controls, thus enabling more effective identification of risk trends.
  - Effective coordination of testing and monitoring activities between first and second lines:
    - Embed majority of testing/monitoring resources in first line to conduct more frequent activities and report results to line of business management and Risk partners.
    - Second line resources to validate and rely on the results of first line testing in order to scale back or reallocate resources.
    - Maintain independent second line testing for high(er) risk regulatory areas.

Where do we go from here?

- **Maintain First Line Accountability Balanced with Strong Second Line Oversight and Challenge**
  - First line should perform its own risk analysis and reporting.
  - First line should regularly conduct risk-focused meetings with its senior management, to include second and third line partners.
  - First line should continue to encourage a culture of self-identification of control issues.
  - Second (and third) lines must actively inspect and challenge overall control environment based on current and planned activities/products.

Closing Comments

- Significant improvements have been made in Enterprise Risk Management governance and reporting processes since the global financial crisis
- Continued importance of Culture, and more specifically Risk Culture
- How to create more role clarity and optimize resources across the first and second lines?
- Conduct risk? How does this get examined? Where does it fit?
- Impending regulatory relief on a number of fronts?

"It's not what you look at that matters, it's what you see."

- Henry David Thoreau