Three Lines of Defense: Working Together to Enhance Business Performance

Rebecca Towne
President, Quadrant Risk Advisory
Topics for Today

1. The Case for Three Lines of Defense
2. Driving Value – Roles and Responsibilities of the Three Lines of Defense *(Warning – there is a quiz)*
3. Combining Three Lines of Defense with a Strong Risk Culture
4. Organizational Structures to Support Three Lines of Defense
5. Examples - Three Lines of Defense Working Together to Protect the Bank
6. Putting It All Together to Enhance Business Performance
Making the Case for Three Lines of Defense

Contributors to poor industry performance during the latest financial crisis include:

- Loan growth and new product/market strategies that were not aligned with banks’ risk appetite or risk-taking capacity
- Incentives that created a strong drive for short-term profit and led to intense pressures to approve risky transactions
- Risks managed in silos, making it difficult to recognize risk interactions and develop a holistic view of risk
The Three Lines of Defense - a Partial Solution

1. **First Line** - Senior management and the front line (including functions providing operational support and technology services)

2. **Second Line** - Risk management functions (including Compliance)

3. **Third line** - Internal Audit
Breakdowns Across the Lines of Defense

- Incentives focused on short-term growth
- Audits based on flawed risk assessments
- Risk Management failed to identify issues
- Warnings ignored by senior management
- Risk Management lacked “teeth”
- Board not informed of risks
- Culture inhibited communication of risks
Do All Banks Need Three Lines of Defense?

- Large banks (generally >$50 B in assets) are required to have a governance framework with three, clearly defined lines of defense.

- Our experience: most banks with >$5 B in assets have established three lines of defense.

- Smaller banks have more flexibility; however:
  - Regulators usually expect to see three lines of defense for compliance risk management.
  - All banks are expected to have a risk governance framework with appropriate checks and balances.
Evaluating Your Risk Governance Framework

In evaluating the formality and resource level of your risk governance framework, consider your bank’s:

- **Growth rate and complexity**
- **Past performance through business cycles**
  - Consider whether performance reflects the bank’s risk management approach, or market and product mix
  - Consider all risk types, as the next major event may be related to information security, fraud, or investments
- **Risk culture**
  - Lack of front line risk ownership or management/board support for risk management requires a higher level of formality and resources
Driving Value – Roles and Responsibilities of the Three Lines of Defense
The 1st Line of Defense – the Front Line

- The first line has the highest level of knowledge of the products, services and processes in their areas – including how to mitigate most risks
- They are also responsible for complying with internal and external rules and regulations
The 1st Line of Defense – Senior Management

- Senior management is part of the 1st line, despite responsibility for oversight to ensure safety and soundness and compliance with laws and regulations.

- Under the three lines of defense model, senior management:
  - Sets the tone-at-the-top that influences the behaviors of the 1st line of defense.
  - Is less transaction focused and more portfolio/total bank focused than the rest of the 1st line of defense.
Contrary to popular belief, risk management’s role is **not** to make work for the 1st line of defense.
The 2nd Line of Defense – The Coordinators

- The 2nd line of defense should be a combination of *watchdog* and *trusted advisor*
- They may also assist in monitoring risks (e.g., compliance)
- In some areas (e.g., risk limits) they need “teeth” and the ability to veto decisions deemed to be inconsistent with the Board’s appetite for risk
- The Chief Risk Officer (or equivalent) should have an open line to the Board (in executive session)
A Real Life Example – Doctors & Patients

- As the 1st line of defense, patients must manage their own risks
- Like the 2nd line of defense, doctors share their expertise on risks; decisions are made by patients
- Doctors rely on patients to provide information that will help in looking for early signs of problems
- Waiting to go to the doctor until there is already a problem reduces their ability to help
- While a horrible thought, having a 3rd line of defense to follow-up on health recommendations would probably help most of us!
An Effective 2nd Line of Defense

To add value, the 2\textsuperscript{nd} line of defense must:

- Understand how the business makes money, to actively challenge initiatives
- Understand the bank’s products and services (although not to the degree of the 1\textsuperscript{st} line) to provide a useful risk perspective
- Engage the 1st line of defense as equals
- Be involved in business meetings – not brought into the loop after decisions have been made
An Effective 2nd Line of Defense

To enhance business performance, the 2nd line of defense should provide *useful* risk information to help the 1st line make decisions.

"Watch out for the pothole!"

Less useful

More useful
The 3rd Line of Defense – the Referees

- Provides independent assurance that the bank’s risk management framework and controls are appropriate and effective

- Should review the entire risk management program (including the 1st and 2nd lines of defense)
An Effective 3rd Line of Defense

To be effective, the 3rd line of defense must:

- Be aligned with the bank’s risk management priorities and risk appetite
- Have a good understanding of the business and risk management, in order to challenge the 1st and 2nd lines credibly
- Have the stature to enforce the timely resolution of audit findings
- Have an open line to the Audit Committee
Just when you thought everything was clear...

<table>
<thead>
<tr>
<th>Position</th>
<th>1st</th>
<th>2nd</th>
<th>3rd</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chief Credit Officer</td>
<td>X</td>
<td>and/or X</td>
<td>X</td>
</tr>
<tr>
<td>Bank Treasurer</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Human Resources</td>
<td>X</td>
<td>and</td>
<td>X</td>
</tr>
<tr>
<td>Loan Review Officer</td>
<td>X</td>
<td>or</td>
<td>X</td>
</tr>
</tbody>
</table>
### Specific Risk Management Responsibilities

<table>
<thead>
<tr>
<th>Process</th>
<th>1st</th>
<th>2nd</th>
<th>3rd</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify risks</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Assess/Measure risks</td>
<td>Within an area</td>
<td>Enterprise-wide</td>
<td>Within each area</td>
</tr>
<tr>
<td>Manage risks</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monitor risks</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Report risks</td>
<td>Management</td>
<td>Management &amp; Board</td>
<td>Board</td>
</tr>
</tbody>
</table>

**Process: 1st**
- Identify risks
- Assess/Measure risks: Within an area
- Manage risks
- Monitor risks
- Report risks: Management

**Process: 2nd**
- Identify risks
- Assess/Measure risks: Enterprise-wide
- Monitor risks
- Report risks: Management & Board

**Process: 3rd**
- Identify risks
- Assess/Measure risks: Within each area
- Monitor risks
- Report risks: Board
Avoiding overlap in responsibilities

- Risk management roles and responsibilities should be defined, such as in an ERM Framework
  - Each line of defense should understand the role of the others as well

- Avoid inefficiencies, such as having separate compliance managers within each business line
  - In all cases, 1st line of defense staff should understand the regulations applicable to their areas

- Risk “liaisons” within business lines (generally at larger banks) should have a reporting line to Risk Management
Combining Three Lines of Defense with a Strong Risk Culture
Who is Defending Whom Against What?

**Reminder:** The 1st line of defense should be defending the Bank against risk —
not defending themselves from the 2nd and 3rd lines of defense.
Combining Three Lines of Defense with a Strong Risk Culture

To be effective, a model of three lines of defense must be supported by a strong risk culture, including:

- Risk ownership and shared responsibility for managing risk
- Agreement on the Bank’s risk profile and appetite
- Inclusiveness – getting the right people involved
- Communication – encouraging escalation of risks
- Accountability
Board and Senior Management Support

A strong risk culture requires a “tone-at-the-top” that is supportive of risk management

- Incentives
  - Incentives based on total bank rather than just individual performance
  - Promotions should also reflect desired behaviors, and penalties have to be applied consistently

- Management and the board have to take recommendations from the 2nd and 3rd lines of defense seriously

- Can’t shoot the messenger
Maintaining Business Line Risk Ownership

One of the challenges in creating a strong 2nd line of defense is maintaining front line risk ownership.

Ways to do this:

- Have line managers self-assess their own risks and controls
- Encourage line managers to identify and monitor their own key risk indicators (KRI) – in addition to Risk Management
- Include line managers on audit issues related to enterprise-wide processes (e.g., vendor risk management), in addition to Risk Management
- Include line management in defining the risk appetite
1st and 2nd Lines – Tips for Working Together

- The 1st and the 2nd lines of defense - *not two decision makers*

- The 2nd line of defense should work with the 1st line to develop appropriate risk management processes, and help to drive:
  - Consistency across the enterprise
  - Risk-based processes
  - Prioritization of risks and controls
  - Alignment with the bank’s risk appetite
Lines of Defense – Tips for Working Together

- A common view of risk across the enterprise can be fostered through an enterprise-wide risk and control self-assessment
  - Focuses all three lines of defense on the most material risks to the Bank
  - Enterprise-wide risk assessment can be considered but not used in place of an Internal Audit risk assessment

- Keeping Risk Management and Internal Audit in the loop as changes are made can create efficiencies and avoid bottlenecks
Organizational Structures to Support Three Lines of Defense
Organizational Structure

A common (and effective) community bank risk governance structure:

- **Board**
  - **Risk Management Committee**
  - **Audit Committee**
  - **Risk Subcommittees** (e.g., ALCO)
    - **1st Line of defense**
      - Business lines
    - **Support Groups**
    - **2nd Line of defense**
      - Compliance
    - **3rd Line of defense**
      - Operational Risk
      - Information Security

**Alternative reporting line**

**May be a combined Audit/Risk Committee**
Can the 1\textsuperscript{st} Line of Defense Also Serve as the 2\textsuperscript{nd} Line?

- Yes, if they don’t mind working 80 hours a week, and probably not for Compliance risk
  - The 2nd line should monitor and communicate new and revised regulations to make it easier for the 1\textsuperscript{st} line of defense to remain in compliance

- For certain risk types (e.g., market and information security risks), the 2nd line brings specialized expertise that may not exist within the business lines
Is an ERM Function Necessary to Have an Effective 2\textsuperscript{nd} Line of Defense?

Not necessarily.

- Large banks are required to have an independent risk management function under the direction of a Chief Risk Officer.

- For smaller community banks, risks may be overseen separately by Compliance and Credit Administration and committees such as ALCO.

- Enterprise-wide risk management processes (e.g., vendor management) can be handled by Operations.
Maintaining Effectiveness without ERM

Without an ERM function it can be difficult to develop a holistic view of risk across business areas and risk types
- Risks are usually reported separately to the Board through risk committees (e.g., ALCO, Credit)

In these cases, management and risk committees should provide effective challenge

Finance functions can help with enterprise-wide risk reporting in lieu of ERM
- Reports should include forward-looking key risk indicators (KRIs) in addition to performance metrics
Examples - Three Lines of Defense Working Together to Protect the Bank
Example – Risk Limits

Board sets risk appetite with input from the 1st & 2nd lines of defense

1st Line of Defense
Accepts risk within limits (may set product-specific limits)

2nd Line of Defense
Monitors/reports limits to the Board
Notifies the 1st line when nearing limits

3rd Line of Defense
Verifies that risks are accurately assessed and reported to the Board

Requests changes to risk limits

Reviews rationale & requests Board approval

Verifies that changes to limits have been reviewed/approved
Example – New Product Proposal

1st Line of Defense

**Identifies opportunities and risks** and brings the 2nd line into the loop

2nd Line of Defense

**Reviews** the proposal for alignment with the risk appetite

3rd Line of Defense

**Verifies** that the risk review process has been followed

Management makes **final decision** (with Board approval, as needed)

**Shares useful information** on risks, needed controls, and required approvals with the 1st line

**Verifies** that necessary controls are in place/effective and approvals met
Putting It All Together to Enhance Business Performance
## Enhancing Business Performance

### Potential Benefits of Three Lines of Defense

- Responsibility for risk management is shared across the enterprise
- Multiple views are considered in making decisions
- Risk-taking is aligned with the Bank’s risk appetite
- The Board receives an independent view of risk

### Potential Impact on Business Performance

- Better risk management and fewer financial “surprises”
- Management’s decisions are more risk-informed
- Risks are taken consistent with the Bank’s capacity, rather than avoided
- Enhanced governance and investor confidence
What questions do you have?

rebecca.towne@quadrantrisk.com

317-566-2112