Session Agenda

- Three Lines of Defense
  - Governance Framework
  - Opportunities and Challenges
  - Roles and Responsibilities

- Accountability Matrix

- Credible Challenge

- Questions

Disclaimer: The views expressed in this presentation are those of the presenter and do not necessarily represent those of KeyCorp or KeyBank N.A.
Three Lines of Defense

- Originated in Financial Services in the early 2000s
- Q4 2014 – OCC published “heightened standards” guidelines on risk governance
- Three units work together to establish an appropriate system to control risk taking
- Board must receive sufficient information to allow for credible challenge of management recommendations and decisions
- Independent Risk Management and Internal Audit have unfettered access to the Board
- The three lines of defense cannot delegate their Framework responsibilities to an external party
Three Lines of Defense

Risk Governance Framework

1st Line of Defense (FLOD)
Front-line Units – directly responsible for identifying and managing risks – Risk owner.
- Revenue Generation
- Operational Support
- Technology Services

2nd Line of Defense (SLOD)
Independent Risk Management – identifies, measures, monitors, controls aggregate risks – independent of FLOD
- Risk Management
- Financial Management
- Human Resources

3rd Line of Defense (TLOD)
Ensures risk governance framework complies with regulatory guidance and is appropriate for the bank’s size, complexity and risk profile
- Internal Audit

4th Line of Defense
- External Auditors

5th Line of Defense
- Regulatory Bodies

1. Risk Pillars: Compliance, Credit, Liquidity, Market, Model, Operational, Reputational, Strategic
Three Lines of Defense

Opportunities and Challenges

Opportunities

- Role and responsibility clarity
- Coordinated and systematic approach to risk management
- Transparency and consistency
- Accountability/risk ownership
- Quality control and risk assurance
- Proactive risk identification and issue detection

Challenges

- Silo-thinking
- Bureaucratic/over-formalized processes
- Duplicity and redundancy
- Inefficiencies
- Talent management
- Maintaining organizational independence
Three Lines of Defense

1st Line of Defense
Front-line Units
Owns and manages risk originated by the business
- Risk identification and assessment
- Risk mitigation
- Monitoring and reporting

2nd Line of Defense
Independent Risk Management
Develops risk framework
- Expert advice, guidance and direction
- Oversight
  - Ensure adherence to risk governance framework
  - Validates known and identifies emerging risks
  - Validates control effectiveness (design and operating)
  - Ensure responsiveness to regulatory change
- Independent perspective and credible challenge

3rd Line of Defense
Independent Audit
Provides assurance to senior management and Board
- Effectiveness of governance, risk management and internal controls, including how 1st and 2nd lines of defense achieve risk management and control objectives
- Independent perspective and credible challenge
Driving Accountability

Ensure accountability by clearly defining roles; evidence and monitor implementation, measure results

**Accountability Model Example – 1st & 2nd Lines of Defense**

<table>
<thead>
<tr>
<th>Front Line Units (1st LOD)</th>
<th>Lines of Business (LOBs)</th>
<th>Business Risk &amp; Controls (Community Bank, Corporate Bank, &amp; KTO)</th>
<th>Independent Risk Management (2nd LOD)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1st Line of Defense (LOD)</strong></td>
<td>Own the risk of the business activities in which you are engaged</td>
<td>Own the risk of the business activities and engage cross-functional stakeholders for an end-to-end view of process prior to implementation and change management</td>
<td>Align resources within the 2nd LOD to provide oversight of compliance and operational risk-taking activities and assessment of risks and findings in the 1st LOD</td>
</tr>
<tr>
<td>Keep 2nd LOD involved with strategies, objectives, and initiatives</td>
<td>Keep 2nd LOD involved with strategies, objectives, and initiatives and changes to processes, products or services</td>
<td>Partner with LOB to keep 2nd LOD involved with strategies, objectives, and initiatives</td>
<td>Maintain a deep understanding of LOB products, services, operations, processes, policies, systems, and procedures in order to identify and understand underlying risk exposures</td>
</tr>
<tr>
<td>Establish LOB-specific compliance and operational risk procedures &amp; processes</td>
<td>Establish LOB-specific compliance and operational risk procedures &amp; processes in conformity with enterprise-wide compliance and operational risk policies &amp; programs</td>
<td>Partner with LOB and 2nd LOD to establish LOB-specific compliance and operational risk procedures &amp; processes in conformity with enterprise-wide compliance and operational risk policies &amp; programs</td>
<td>Establish, educate, and communicate enterprise-wide compliance and operational risk policies &amp; programs</td>
</tr>
<tr>
<td>Distribute applicable reports to the 2nd LOD and cascade Tier II committee reports as appropriate</td>
<td>Distribute applicable reports to the 2nd LOD and cascade Tier II committee reports as appropriate</td>
<td>Partner with LOB to distribute applicable reports to the 2nd LOD and cascade Tier II committee reports as appropriate</td>
<td>Ensure appropriate representation of each MLOB in the Compliance Risk Committee and Operational Risk Committee and disseminate materials to central point of contact as identified by the MLOB</td>
</tr>
<tr>
<td>Establish periodic LOB risk meeting cadence, as appropriate</td>
<td>Establish management meeting cadence with MLOB leader and their direct to provide update and set priorities</td>
<td>Partner with LOB to escalate significant risks to 2nd LOD in accordance with the ERM Policy</td>
<td>Approve significant initiatives, products, third party vendors, and AML high risk clients</td>
</tr>
<tr>
<td>Escalate significant risks, initiatives, products, third party vendors, and AML high risk clients to 2nd LOD</td>
<td>Escalate significant risks, initiatives, products, third party vendors, and AML high risk clients to 2nd LOD in accordance with the ERM Policy</td>
<td>Input risk, control, and test via the Risk and Control Self-Assessment (RCSA) module in the GRC system</td>
<td>Analyze, assess, and decision whether 1st LOD practices are within the corporation’s risk appetite/approach, identifying and escalating risks as appropriate</td>
</tr>
<tr>
<td><strong>Accountability Topics Covered</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Inter-LOD Interaction
- Identify and Assess Risks
- Understand Applicable Laws, Regulations, Rules, Standards and Industry Practices
- Implement and Execute Controls
- Self-assessment Control Testing
- Findings, Remediation Plans, Exception Requests and Escalation
- Reporting
- Regulator Interaction

Page 7
Three Lines of Defense

“One Risk” SLOD partnering to effectively support FLOD

“One Risk” Approach

- Provide a single communication point for FLOD executives for an aggregate risk view:
  - Critical Issues
  - Risk Profile
  - Strategic Initiatives
- Engage all risk partners in group dialogue to identify and address respective risk issues collectively
- Deliver risk management capabilities that drive client success within risk/reward parameters within banks risk appetite
- Individual risk disciplines maintain day-to-day responsibility for executing program level activities
- Critical success factor is for senior leadership of the LOB and Risk Management to embrace a culture of Risk vs. Rewards

Expected Outcomes

Risk management a market differentiator

Increased leverage of cross functional risk SME’s

Reduced portfolio risk exposure – maintain risk appetite

Reduced friction & improved consistency

Increased leverage of Business and Risk Executive Management team

Improved risk management effectiveness
Credible Challenge

“The CEO and front-line units demonstrate support by welcoming credible challenges from independent risk management and internal audit.” — Heightened Standards

The “credible challenge” standard requires the Board to obtain a thorough understanding of the institution’s risk profile, to ask probing questions of management and to ensure senior management’s actions prudently address risks.

Expectations of the Board:

➢ Actively oversee the bank’s risk-taking activities
➢ Hold management accountable for adhering to the Risk Framework
➢ Critically evaluate management’s recommendations and decisions
  • Question, challenge and oppose (as necessary) management’s proposed actions that may exceed risk appetite or threaten safety and soundness
Credible Challenge

For SLOD, credible challenge involves continuously identifying and assessing the bank’s material aggregate risks, then leveraging the risk assessments to determine what, if any, actions are required to strengthen risk management or reduce risk to maintain the bank’s desired risk profile.

Factors to consider for effectiveness:

- Authority (granted through Board approval of governance structure)
- A credible SLOD (persuasive and believable)
- Adequate skills and expertise within the SLOD
- Cohesive relationship between FLOD and SLOD
- Well-defined challenge processes (policies/procedures)
- Effective issue tracking and escalation
- Issue acknowledgement
- Sense of urgency and focus
- SLOD is effective at driving change
- SLOD reporting structure is independent from FLOD
Review and challenge is appropriate for numerous activities across the franchise. SLOD should take a risk-based approach, focusing efforts on those activities required by regulatory guidance and those most impactful to the LOB and organization’s risk profile.
Credible Challenge

Questions
- How did you come to that decision?
- What outcome are you trying to achieve?
- Share with me your thought process.
- Do you understand what the risks are?
- What are the assumptions?
- Does this fit within the Framework and Strategic Plans?

Things to Consider:
- Avoid being too close or too far from the FLOD
- Take a common sense approach; don’t over complicate things
- Drive two-way dialogue (engagement and interchange)
- Ensure transparency
- Ensure processes are documented in policies and procedures
- Evidence review and challenge through detailed documentation

Source: Setting up a second line of defense and the art of challenge - McGladrey

The art of effective challenge
Scope and depth
- Conceptual – looking forward. Apply industry knowledge to business. Cross-correlate and compare outcomes. High complexity and criticality
- Transactional – looking back. Issues identified, meetings held. Low complexity and criticality.
Credible Challenge – Evidencing Activities

- **What to Document:**
  - What was reviewed?
  - What was the review period?
  - What was identified?
  - Who were discussions held with?
  - What was the outcome (i.e., agreement, escalation, resolution, etc.)

- **Where to Document:**
  - Governance Risk Compliance (GRC) application
  - Customized review and challenge templates
  - Feedback memo
## Credible Challenge – Evidencing Activities

### GRC Documentation Example

<table>
<thead>
<tr>
<th>Example</th>
<th>Challenge Type</th>
<th>What was challenged?</th>
<th>Discussion &amp; Resolution with LOB</th>
<th>Escalation of Challenge</th>
</tr>
</thead>
<tbody>
<tr>
<td>Escalation to Risk Discipline Executive – No Change Required</td>
<td>Inherent Risk</td>
<td>Inherent Risk rating of Moderate appears to be low given the supporting rationale. Emerging risks relative to customer regulatory compliance is significant in the business area and should ultimately impact the inherent risk. Major changes in processes and controls will need to be made to comply with increasing regulatory changes. In addition, RCSA aggregation shows the Inherent Risk rating should be Moderate/High based upon risk ratings in GRC.</td>
<td>Risk Management discussed the Inherent Risk challenge with Joe Smith, Retail Banking Executive. He did not agree that the Inherent Risk of business was being impacted by the regulatory factors around customer compliance.</td>
<td>Challenge was escalated to the Chief Compliance Officer. The matter was discussed between Chief Compliance Officer and Joe Smith and the resolution was the Inherent Risk rating would remain as Moderate for this quarter, however, next quarter the rating would be raised to Moderate/High because the regulatory factors affecting customer compliance will be better understood as to how the issues will be affecting the business area.</td>
</tr>
<tr>
<td>Escalation to Tier II Committee – Changes Required</td>
<td>Management Control &amp; Effectiveness</td>
<td>Risk Management challenged the MCE rating of Effective based on review of open RRG findings and regulator MRAs. Specifically, control gaps identified were around credit card workouts and management reporting/oversight. Risk Management feels the appropriate MCE rating based on these risk factors should be Needs Improvement.</td>
<td>Discussion held with Mary Smith, Loan Services Executive. She disagreed that the open findings have that much of a significant impact to the MCE rating. Remediation plans are on track for closure by 12/31/15.</td>
<td>The challenge was escalated to the Chief Operational Risk Officer. Discussions were held, but LOB continued to disagree that the MCE rating should be downgraded. The disagreement was escalated to the Operational Risk Committee on 10/07/15 for further discussion with LOB management. After discussion at ORC, it was determined that rating should be lowered to Needs Improvement to appropriately represent the magnitude of the control gaps in the findings. LOB changed rating to Needs Improvement and added commentary to the profile to support such a rating.</td>
</tr>
<tr>
<td>No Escalation</td>
<td>Residual Risk</td>
<td>Additional justification is needed around the Moderate rating. LOB is within risk appetite on all risk metrics (tolerances and KRIs). Please add commentary around metrics within rationale for residual risk.</td>
<td>Discussion held with Bob Smith, Finance Executive and he agreed and added the additional justification.</td>
<td>Not Applicable</td>
</tr>
</tbody>
</table>
Credible Challenge – Evidencing Activities

Sample Review & Challenge Template – Business Initiatives

OPERATIONAL RISK MANAGEMENT TEAM
Review and Challenge

<table>
<thead>
<tr>
<th>Initiative Type:</th>
<th>New Product/Service</th>
<th>New Process</th>
<th>Change in Product/Service</th>
<th>Change in Process</th>
<th>Product Review</th>
<th>Other</th>
</tr>
</thead>
</table>

**SUMMARY:**

Identified Risks - use the space below to identify Operational Risks related to this product, service or process:

<table>
<thead>
<tr>
<th>Identified Risk:</th>
<th>Inherent Risk</th>
<th>Risk Description</th>
<th>How is Risk Mitigated?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Operational Risk Recommendation - use the space below to identify recommendation:

<table>
<thead>
<tr>
<th>Recommendation Description</th>
<th>To Whom Recommendation Made (Employee Name)</th>
<th>Date Recommended</th>
<th>Target Date</th>
<th>Escalation Required</th>
<th>Comments and Conclusion</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Conclusion:
Credible Challenge

- Understand your role as SLOD
- Build a collaborative relationship with FLOD
- Set agreed upon SLAs for challenge activities
- Leverage active listening skills
- Over Communicate – continuously and frequently
- Gain a sound understanding of FLOD processes, procedures and policies before drawing conclusions; allow for FLOD to clarify, refute
- Partner within SLOD – ensure one coordinated voice or perspective back to FLOD
- Fully explain rationale for credible challenge conclusions
- Thoroughly document challenge activity – Perception: if it isn’t documented, it wasn’t done!
- Remember, credible challenge is about assessing for effectiveness; it’s okay to not find deficiencies
Sources

- Setting up a second line of defense and the art of challenge (July 2015), McGladrey
- Risk Governance, Visual Memorandum on Guidelines Adopted by the OCC (Nov. 7, 2014), Davis Polk
- Financial Stability Institute: Occasional Paper No 11 – The “four lines of defence model” for financial institutions (December 2015), Bank for International Settlements