INTRODUCTION TO OPERATIONAL RISK

Session 2

TODAY’S INSTRUCTOR

Phyllis Segal

phyllis@segal.org

- RMA Faculty – Operational Risk
- Member of RMA’s Operational Risk Council

SESSION 2 - OBJECTIVES

- Review Homework
- Operational Risk Management Tools
  - RCSA
  - KRI
  - Loss Reporting and Analysis
  - Reporting Framework
- Practical approaches to ORM for a financial institution
### CASE 2 - BANK OF AMERICA

- Two employees of Bank of America in Austin, TX pleaded guilty to stealing $2.6 million from the bank and five of its predecessors over a 23-year period.

- The women stole the money in small increments (typically $2,500) over a long period of time by taking cash from the vaults they controlled and manipulating bank records. One of the women was a customer service manager, while the other was teller manager of a drive-through branch several blocks away.
CASE 2 - BANK OF AMERICA (CONT.)

- Prosecutors said that the scheme involved false accounting and manipulation of records of cash transfers between the vaults of the two branches, and that their approach changed over time as the banks changed hands and the women gained additional responsibilities.
- The women had reputations as tough, by-the-book supervisors. Over the years, they refused promotions and transfers, and planned their vacations to ensure that the fraud was not uncovered.

CASE 2 - BANK OF AMERICA (CONT.)

- Their strategies worked until Bank of America introduced a new computer system which identified differences between vault cash and ledger balances.

MINI CASE STUDIES – SOLUTIONS

<table>
<thead>
<tr>
<th>Case</th>
<th>Weakness</th>
<th>OR Loss</th>
<th>Regulatory Category 1</th>
<th>Regulatory Category 2</th>
<th>Case</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bank of America &amp; predecessors</td>
<td>Internal Fraud</td>
<td>$2.6 million</td>
<td>Internal Theft and Fraud</td>
<td>Theft and Fraud</td>
<td>Bank of America &amp; predecessors</td>
</tr>
</tbody>
</table>
CASE 7 - MUNICIPAL CREDIT UNION

• Fifteen million dollars was illegally withdrawn from accounts with the Municipal Credit Union of New York City in the days after the tragic events of September 11, 2001.

• The Credit suffered a computer failure after the collapse of the World Trade Center towers, and allowed its clients limited access to its automated teller machines as a service during a difficult time. The Credit Union was across the street from the World Trade Center and lost its connection to the New York Cash Exchange ATM network. The network had no way of insuring that when credit union clients withdrew money from ATM machines that there was sufficient money in their accounts to cover the transactions.

• Arrest warrants were issued for more than one hundred people who withdrew $7,500 or more beyond what was in their accounts, and an estimated 4,000 people were suspected of smaller frauds. All of those investigated overdrew their accounts by at least $1,000 and refused offers from the city to pay back their overdrafts through loans at reduced interest rates.
CASE 7 - MUNICIPAL CREDIT UNION

- According to the Credit Union it went out of its way to create an atmosphere of orderliness during a time of great trauma and was victimized by people who took advantage of the situation.

MINI CASE STUDIES – SOLUTIONS

<table>
<thead>
<tr>
<th>Case</th>
<th>Category</th>
<th>Loss</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AmSouth Bank</td>
<td>BSA/AML, Compliance</td>
<td>$1 million</td>
<td>Execution, Delivery, and Process Management Monitoring and Reporting</td>
</tr>
<tr>
<td>Bank of America &amp; predecessor</td>
<td>Internal Fraud</td>
<td>$2.6 million</td>
<td>Internal Theft and Fraud Theft and Fraud</td>
</tr>
<tr>
<td>Carrollton Bancorp &amp; BSB Bankcorp</td>
<td>External Fraud</td>
<td>$12.4 million</td>
<td>External Theft and Fraud Theft and Fraud</td>
</tr>
<tr>
<td>CIBC</td>
<td>Unreasonable Process</td>
<td>$3 million</td>
<td>Execution, Delivery, and Process Management Transaction Capture, Execution, and Maintenance</td>
</tr>
<tr>
<td>Citizens Bank</td>
<td>Internal Fraud</td>
<td>$8 million</td>
<td>Client, Products, and Business Practices Scam, Deception, and Fraud</td>
</tr>
<tr>
<td>Compass Bank</td>
<td>Employment Practices</td>
<td>$1 million</td>
<td>Employment Practices and Workplace Safety</td>
</tr>
<tr>
<td>Municipal Credit Union</td>
<td>Physical Damage</td>
<td>$15 million</td>
<td>Business Disruptions and Systems Failures</td>
</tr>
<tr>
<td>National Penn Bancshares</td>
<td>Internal Fraud</td>
<td>$11.2 million</td>
<td>Internal Theft and Fraud Theft and Fraud</td>
</tr>
</tbody>
</table>

MODULE 4 OBJECTIVES

- Identify the basic set of operational risk tools currently used and being developed by the industry.
- Identify each operational risk tool in relation to the risk management process.
- Compare and contrast the attributes of each tool.
- Discuss the benefits and the challenges of implementing each tool.
OPERATIONAL RISK MANAGEMENT TOOLS

- Risk and control self-assessment.
- Key risk indicators.
- Loss reporting and analysis tools.
- Risk management reporting frameworks.

THE RISK MANAGEMENT PROCESS

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Define OR categories.</td>
<td>Formulate definition.</td>
<td>Institute risk &amp; control assessments.</td>
<td>Define measures of risk (EL &amp; UL).</td>
<td>Define risk transfer approach.</td>
<td>Establish how to incorporate OR into existing RORAC, etc.</td>
</tr>
</tbody>
</table>

RISK MANAGEMENT PROCESS – RCSA
TOOL 1: RISK AND CONTROL SELF-ASSESSMENT

- **What is it?**
  - Identifies and defines material risks.
  - Provides a relative assessment of severity and frequency of risks.
  - Identifies control weaknesses.
  - Documents actions.
  - Monitors progress.
  - Formalizes escalation criteria.

RISK AND CONTROL SELF-ASSESSMENT

- A great starting point – straightforward and relevant.
- Fosters risk discovery, ownership, and communication.
- Helps institutionalize a set of standard categories.
- Identifies control weaknesses and establishes consensus on required changes.
RISK AND CONTROL
SELF-ASSESSMENT – BENEFITS (CONT.)
• Establishes an ongoing, forward-looking process.
• Helps to facilitate effective reporting.
• Offers holistic, top-down insight.
• Can engage the organization and keep it engaged.
• Can help build institutional memory.

RISK AND CONTROL
SELF-ASSESSMENT – CHALLENGES
• Resource intensive.
• Subjective.
• Difficult to get buy-in and make it a part of the culture.
• Can be tricky to make the output relevant to each user group.

RISK AND CONTROL
SELF-ASSESSMENT – CHALLENGES
• Difficult to demonstrate progress and achievements (i.e., risks avoided).
• Can feel static after multiple iterations.
RISK MANAGEMENT PROCESS – KEY RISK INDICATORS

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Define OR categories</td>
<td>Formulate risk definitions</td>
<td>Institute risk &amp; control assessments</td>
<td>Define measures of risk (EL &amp; UL):</td>
<td>Define risk transfer approach</td>
<td>Define transfer approach to integrate OR into existing processes</td>
</tr>
<tr>
<td>• Define OR categories</td>
<td>• Define risk definitions</td>
<td>• Institute risk &amp; control assessments</td>
<td>• Define measures of risk (EL &amp; UL):</td>
<td>• Define risk transfer approach</td>
<td>• Assess and execute controls</td>
</tr>
<tr>
<td>• Include risk with MR, CR, and bus/strat.</td>
<td>• Formulate risk definitions</td>
<td>• Institute risk &amp; control assessments</td>
<td>• Define measures of risk (EL &amp; UL):</td>
<td>• Define risk transfer approach</td>
<td>• Establish specific OR performance mechanisms</td>
</tr>
<tr>
<td>• Define “loss”</td>
<td>• Institute risk &amp; control assessments</td>
<td>• Define measures of risk (EL &amp; UL):</td>
<td>• Develop risk transfer approach</td>
<td>• Assess and execute controls</td>
<td>• Establish specific OR performance mechanisms</td>
</tr>
</tbody>
</table>

TOOL 2: KEY RISK INDICATORS

• What are they?
  – Measures that effectively track an aspect of a significant risk:
    • Identify objective leading and lagging measures/proxies for each risk category.
    • Establish reporting to compare across time and business lines (and even other companies).
    • Establish bands of acceptance/appetite and trigger levels for review and/or action.
    • Generate assessment based on level of indicators against frame of reference.

KEY RISK INDICATORS EXAMPLE 1

• Traffic volume is an indicator of how dangerous it is to cross the road.
• Does higher traffic volume make crossing more dangerous or less?
KEY RISK INDICATORS EXAMPLE 1 (CONT.)

• What other factors might influence the level of risk?

Commentary:
Credit scores are decreasing consistently and charge offs are increasing as trends. However, the numbers involved are still very small when taken in the context of the loan portfolio and still within tolerance. The volumes should be watched because the numbers could grow quickly.

KEY RISK INDICATORS EXAMPLE 2

<table>
<thead>
<tr>
<th>Credit Scores</th>
<th>Charge Offs (#)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2008-2009</td>
<td>2009-2010</td>
</tr>
<tr>
<td>630/2009</td>
<td>630/2010</td>
</tr>
<tr>
<td>850</td>
<td>705</td>
</tr>
</tbody>
</table>

Commentary:
Credit scores are decreasing consistently and charge offs are increasing as trends. However, the numbers involved are still very small when taken in the context of the loan portfolio and still within tolerance. The volumes should be watched because the numbers could grow quickly.

KEY RISK INDICATORS

 Processing Risks
 Conduct Risks
 External Risks

Start-to-finish process metrics covering:
• Execution
• Settlement
• Accounting/custody

Incident metrics
• Complaint metrics

Outside factors such as:
• Attacks and thefts
• Other near misses
• Natural disasters
• etc.

For each indicator, establish the main dimensions of frequency and severity by business area and/or process: number, size, timing, etc.
EXAMPLES OF KEY RISK INDICATORS

**People**
- HR training
- Turnover rate
- Experience level
- Staff profiling

**Process**
- Customer satisfaction
- Employee satisfaction
- Automation level
- Reconciliations outstanding

**Technology**
- Customer access
- Availability/ stability
- Level of change
- Capacity utilization

EXAMPLE: RMA/RISKBUSINESS
TOP 18 KRIS FOR RETAIL LENDING

**Process Risk:**
- Number of new loans with loan/security documentation out of order.

EXAMPLE: RMA/RISKBUSINESS
TOP 18 KRIS FOR RETAIL LENDING (CONT.)

**Fraud Risk:**
- Number of exceptions to lending policy.
- Percent of loans that default early.
- Percent of applications originating from outside (i.e., brokers).
- Number of lenders or units that exceed sales target by a predefined percentage.
EXAMPLE: RMA/RISKBUSINESS
TOP 18 KRIS FOR RETAIL LENDING (CONT.)

• Information Security Risk:
  – Number of third parties/vendors who are dealing with high, materiality, sensitive customer information
  – Number of attacks reported (spam, hacking, phishing attacks)
  – Percent of 3rd parties with info security exceptions or concerns.
  – Access rights to applications by staff: number of reviews beyond threshold

• Compliance Risk:
  – External audit points open, overdue, or raised.
  – Number of compliance-related complaints.
  – Compliance issues raised by external professional bodies.
  – Number of policies and procedures not reviewed within threshold.

• Account Reconciliation Risk:
  – Number open items beyond threshold.
  – Reconciliation differences (total gross value of open items beyond threshold)

• Change Risk:
  – Volume increase/decrease by product.
  – Number of regulatory changes during period.
  – Number of new products or substantial changes.
### KEY RISK INDICATORS – BENEFITS

- KRI are dynamic.
  - They are objective and transparent.
  - They can track levels of risk over time.
  - They can be predictive and serve as a warning indicator.

### KEY RISK INDICATORS – CHALLENGES

- Making the KRI program comprehensive.
- Making the KRI program causative.
- Eliminating noise/avoiding the activity trap.
- Avoiding duplication.

### RISK MANAGEMENT PROCESS – LOSS REPORTING

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Define OR, Control, Change, and Off-shore</td>
<td>Formulate definitions, objectivity, and transparency</td>
<td>Define risk and control assumptions</td>
<td>Analyze risk, controls, and transparency</td>
<td>Define risk transfer approach</td>
<td>Benchmarking and comparative analysis</td>
</tr>
<tr>
<td>Define Incentives and PR, CK, and Incentives, Off-shore</td>
<td>Formulate definition and transparency, objectivity</td>
<td>Define risk management</td>
<td>Analyze risk, controls, and transparency</td>
<td>Define risk transfer approach</td>
<td>Benchmarking and comparative analysis</td>
</tr>
<tr>
<td>Define OR, Control, Change, and Off-shore</td>
<td>Formulate definitions, objectivity, and transparency</td>
<td>Define risk and control assumptions</td>
<td>Analyze risk, controls, and transparency</td>
<td>Define risk transfer approach</td>
<td>Benchmarking and comparative analysis</td>
</tr>
</tbody>
</table>

- Establish how to incorporate OR into existing RORAC, etc.
- Establish proper transfer pricing of premium and EL/captive mechanisms
- Establish specific OR performance mechanisms
### TOOL 3: LOSS REPORTING AND ANALYSIS

- **What is it?**
  - Answers the question, how much did we lose?
  - Compares across time and business lines.
  - May include information on nonfinancial costs and near-misses as well as financial costs.
  - Generates assessment based on level of loss.

### LOSS REPORTING & ANALYSIS

<table>
<thead>
<tr>
<th>Processing risk</th>
<th>Q3 loss report</th>
<th>Detailed report – charge offs</th>
<th>Charge offs ($) ‘000</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Q4 2009</td>
<td>Q1 2010</td>
<td>Q2 2010</td>
</tr>
<tr>
<td>Comm.</td>
<td>23.8</td>
<td>25.6</td>
<td>24.3</td>
</tr>
<tr>
<td>Resid.</td>
<td>270.2</td>
<td>247.5</td>
<td>305.7</td>
</tr>
<tr>
<td>Cons.</td>
<td>0.1</td>
<td>1.5</td>
<td>2.5</td>
</tr>
<tr>
<td>Total</td>
<td>294.1</td>
<td>274.6</td>
<td>332.5</td>
</tr>
</tbody>
</table>

### LOSS REPORTING AND ANALYSIS – BENEFITS

- Provides primary risk data of interest to business.
- Objective and transparent.
- Raises awareness and can spark analysis and action.
- Can serve as input for statistical measures of risk such as expected and unexpected loss.
LOSS REPORTING AND ANALYSIS – BENEFITS (CONT.)

• Increases awareness of losses and trends.
• Provides input for examining causative relationships.
• Metrics can be used as performance criteria.

LOSS REPORTING AND ANALYSIS – CHALLENGES

• Completeness and reconciliation to financials.
• Avoiding duplication of effort.
• Process reengineering of sub-processes.
• Accounting changes.
• Discovery issues.

THREE TYPES OF OR DATA

<table>
<thead>
<tr>
<th>Lagging Measures</th>
<th>Leading Measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>RISKS</td>
<td>Risk Assessment Data</td>
</tr>
<tr>
<td>KRI Framework (statistics that indicate a risk has occurred)</td>
<td>(assessments that foresee potential risks)</td>
</tr>
<tr>
<td>Losses (financial impact of risk)</td>
<td>KRI Framework (statistics that indicate a risk could occur)</td>
</tr>
</tbody>
</table>
INDUSTRY INITIATIVES

• RiskBusiness – Loss Data Consortium Service allows participating firms to view both individual loss event reports as well as aggregate loss data summaries. [www.riskbusiness.com](http://www.riskbusiness.com)

• ORX – Industry operational risk loss data pooling for benchmarking and/or risk quantification: [www.orx.org](http://www.orx.org).

RISK MANAGEMENT REPORTING FRAMEWORK

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>- Define OR categories</td>
<td>- Formulate definitions</td>
<td>- Formulate risk categories</td>
<td>- Formulate risk analysis</td>
<td>- Define risk transfer approach</td>
<td>- Establish how to incorporate OR into existing RORAC, etc.</td>
</tr>
<tr>
<td>- Define boundaries, OR, CR, and business risk</td>
<td>- Formulate risk categories</td>
<td>- Engage in loss event reporting (internal &amp; external events)</td>
<td>- Engage in loss event reporting</td>
<td>- Price and execute coverage</td>
<td>- Establish OR performance measures</td>
</tr>
<tr>
<td>- Define loss events</td>
<td>- Engage in loss event reporting</td>
<td>- Engage in loss event reporting (internal &amp; external events)</td>
<td>- Engage in loss event reporting</td>
<td>- Ensure proper transfer pricing of premium and EL/captive mechanisms</td>
<td>- Establish specific OR performance measures</td>
</tr>
<tr>
<td>- Define loss reporting</td>
<td>- Engage in loss event reporting</td>
<td>- Engage in loss event reporting (internal &amp; external events)</td>
<td>- Engage in loss event reporting</td>
<td>- Ensure proper transfer pricing of premium and EL/captive mechanisms</td>
<td>- Establish specific OR performance measures</td>
</tr>
<tr>
<td>- Define loss recording</td>
<td>- Engage in loss event reporting</td>
<td>- Engage in loss event reporting (internal &amp; external events)</td>
<td>- Engage in loss event reporting</td>
<td>- Ensure proper transfer pricing of premium and EL/captive mechanisms</td>
<td>- Establish specific OR performance measures</td>
</tr>
</tbody>
</table>

TOOL 4: RISK MANAGEMENT REPORTING FRAMEWORK

• What is it?
  - Standardized template for periodic and point-in-time reporting of risk management results and environment.
  - Consolidates input from various sources into a summary suitable for its intended audience.
  - Used to facilitate review and subsequent determination and documentation of actions to be taken.
Q3 2010 PROCESSING RISK REPORT – LENDING

ABC Bank Limited

Risk Summary
As of 9/30/2010

Lending Business

Overall Risk Rating - LOW Approval

<table>
<thead>
<tr>
<th>Business Mgmt. Risk Mgmt.</th>
<th>Charge Offs</th>
<th>Action Item Alert</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q4 2009</td>
<td>Q1 2010</td>
<td>Q2 2010</td>
</tr>
<tr>
<td>Open Lending High Risk Items Status</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Com.</td>
<td>23.8</td>
<td>25.6</td>
</tr>
<tr>
<td>Resid.</td>
<td>270.2</td>
<td>247.5</td>
</tr>
<tr>
<td>Cons.</td>
<td>0.1</td>
<td>1.5</td>
</tr>
<tr>
<td>Total</td>
<td>294.1</td>
<td>274.6</td>
</tr>
</tbody>
</table>

Key Risk Indicators (KRIs)
Environmental Factors (EFs)

As at 9/30/2003 | As at 9/30/2004 | Average Rating | As at 9/30/2009 | As at 9/30/2010 | Average Rating |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Credit Scores</td>
<td>850</td>
<td>700</td>
<td>775</td>
<td>LOW</td>
<td></td>
</tr>
<tr>
<td>Custom e r Sa tisfa ction</td>
<td>37</td>
<td>3.5</td>
<td>LOW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Charge Offs</td>
<td>02</td>
<td>1</td>
<td>LOW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Loan Growth</td>
<td>50</td>
<td>500</td>
<td>225.0</td>
<td>MOD</td>
<td></td>
</tr>
</tbody>
</table>

Commentary:
Credit scores are decreasing consistently and charge offs are increasing as trends. However, the Customer satisfaction is a problem. The marketing focus groups indicate that we are perceived as numbers involved are still very small especially when taken in the context of the loan portfolio. The cherry picking in the market and as being inflexible. The sales people are clamoring for additional volumes should be watched because the numbers could grow quickly.

Environmental Factors (EFs)

Q3 2010 Credit Scores

Q3 2010 Charge Off Rates

Q3 2010 Loan Growth

Q3 2010 Customer Satisfaction

RISK MANAGEMENT REPORTING FRAMEWORK – BENEFITS

- Brings together multiple views to facilitate a comprehensive summary and analysis of risk.
- Brings discipline, formalization, escalation, transparency, accountability, and responsibility to the process.
- Facilitates review and provides a basis for sound decision making.

- Enables comparison over time across businesses and risk types.
- Provides documentation of the company’s risk management efforts.
RISK MANAGEMENT REPORTING FRAMEWORK – CHALLENGES

• Requires multiple inputs and can thus be resource intensive and difficult to access.
• Can be difficult to discern the level of detail required by various constituencies.
• Can be difficult to ensure that important data stands out.
• Only as good as the quality of the management attention it receives.

REVIEW OF MODULE 4 OBJECTIVES

• Identify the basic set of operational risk tools currently used and being developed by the industry.
• Identify each operational risk tool in relation to the risk management process.
• Compare and contrast the attributes of each tool.
• Discuss the benefits and the challenges of implementing each tool.

MODULE 5 OBJECTIVES

• Consider practical approaches for a financial institution - ways to add value through the operational risk management discipline.
• Develop a course of action for when you return to the real world.
ORM CHALLENGES FOR FINANCIAL INSTITUTIONS

• No immediate regulatory imperative:
  – Lots of specific operational risk-related requirements, but nothing related to a more proactive and broader initiative.

• No predominant model to follow.

• Large bank approaches not always practical for smaller institutions.

ORM CHALLENGES FOR FINANCIAL INSTITUTIONS (CONT.)

• Limited resources and management focus.

• Difficult to quantify value creation.

ORM BENEFITS FOR FINANCIAL INSTITUTIONS

• ORM provides opportunities to:
  – Stay ahead of an increasing and evolving set of risks.
  – Improve risk awareness across the organization.
  – Ensure that decisions on risk tolerance are made by the right people with the right information in front of them.
  – Ensure that various organizational levels are on the same page regarding risk tolerance and mitigation.
ORM BENEFITS FOR FINANCIAL INSTITUTIONS (CONT.)

- Enhance corporate governance and provide evidence of appropriate risk management.
- Strengthen institutional memory and knowledge.
- Develop and sustain a culture of risk management effectiveness.

MCKINSEY & COMPANY STUDY – BEST PRACTICES

1. Strong governance with clear ownership of operational risks.
2. Clear understanding of where operational risks are concentrated.
3. Alignment of risk controls with the defined appetite and tolerance.

4. Effective management of information.
5. True inclusion of operational risk practitioners in decisions about strategic or organizational changes.
POTENTIAL OBJECTIVES OF AN ORM PROGRAM

• Clear accountability for managing operational risk.
• Identification, evaluation, and acceptance of material risks.
• Open communication up, down, and across the organization.
• More informed decision-making.

POTENTIAL OBJECTIVES OF AN ORM PROGRAM

• Reduction of cost (monetary and non-monetary) through prevention of foreseeable losses.
• Resource commitment proportional to business benefits.

SO HOW DO WE GET THERE?

• “Begin with the end in mind.”
  – Stephen Covey, 7 Habits of Highly Effective People
PRACTICAL APPROACH 1

• Start with the Basel Committee’s paper on Principles for the Sound Management of Operational Risk (June 2011):

• Forget that it was written by regulators; treat it as if it were written by a consultant engaged by your bank to recommend best practices.

PRACTICAL APPROACH 1 (CONT.)

• Make a list of the items that would benefit your institution and another list of items that are inappropriate.

• Adjust those that would benefit your institution to reflect what will work best in your culture; don’t do the things that don’t add value.

PRACTICAL APPROACH 2

• Develop an operational risk management framework:
  – Define operational risk.
  – Include accountabilities for managing op risk from the board on down.
    ◦ Consider formation of board/management-level committees.
PRACTICAL APPROACH 2 (CONT.)

• Develop an operational risk management framework:
  – Include corporate-level principles for managing operational risk.
  – Define approving framework at the board level.
  – Stay high-level and practical; ensure compliance with the framework.

PRACTICAL APPROACH 2 (CONT.)

• Develop an operational risk management framework:
  – Remember that the purpose is to create “tone at the top.”
  – Communicate throughout the organization.

PRACTICAL APPROACH 3

• Keep the language simple:
  – Communicate, don’t impress.
  – Choose internal jargon over industry jargon every time.
  – Reinforce that your program is homegrown and tailored to the institution’s needs.
  – Where possible, draw parallels to credit risk management.
IS MANAGING OPERATIONAL RISK ANY DIFFERENT FROM MANAGING CREDIT RISK?

• Clear accountability for managing risk.
• Identification, evaluation, and acceptance of material risks.
• Open communication up, down, and across the organization.
• More informed decision-making.

IS MANAGING OPERATIONAL RISK ANY DIFFERENT FROM MANAGING CREDIT RISK? (CONT.)

• Reduction of cost (monetary and non-monetary) through prevention of foreseeable losses.
• Resource commitment proportional to business benefits.

CREDIT RISK VS. OPERATIONAL RISK DIFFERENCES

• Credit risk is accepted knowingly; operational risk exposure not always accompanied by awareness.
• Credit risk acceptance is limited based on explicit authority; operational risk can be taken on by anyone.
• Credit risk is generally quantifiable; operational risk is more difficult to quantify.
PRACTICAL APPROACH 4

• Make a risk self-assessment process the centerpiece of your ORM program:
  – Have each area develop a list of operational risks, using a set of provocative questions to help people think of risks.
  – Conduct a rudimentary evaluation of the risks identified.
  – Identify a small number of material risks in each business unit.

PRACTICAL APPROACH 4 (CONT.)

• Make a risk self-assessment process the centerpiece of your ORM program:
  – Evaluate and document risks in terms of description, ratings, controls, monitoring activities, suggested changes, etc.
  – Repeat the process at least annually.

PRACTICAL APPROACH 5

• Focus your self-assessment process on risk evaluation, not on evaluation of controls:
  – Control evaluation is very important, but it will not capture and hold the attention of management the way risk evaluation will.
  – The gap in most organizations (and hence the value opportunity) is in proactive thought about risk exposures and whether all levels are comfortable with how they are managed.
PRACTICAL APPROACH 5 (CONT.)

• Focus your self-assessment process on risk evaluation, not on evaluation of controls:
  – A risk management focused self-assessment will lead to greater awareness and oversight of control activities.
  – Note: this is not how RCSA is typically done.

PRACTICAL APPROACH 6

• Report periodically to board and management committees on top exposures and material changes:
  – Use risk ratings to identify categories of top risks and report on the risks:
    • Expected case (frequency/severity ratings).
    • Realistic worst case (stress loss/adequacy of controls ratings).
  – Keep level of detail appropriate to the audience.

PRACTICAL APPROACH 6 (CONT.)

• Report periodically to board and management committees on top exposures and material changes:
  – Facilitate committee discussion of top risks and level of comfort with how they are managed.
  – After the first round or two, shift focus to what has changed since prior report.
  – Design process to identify increasing and emerging risks.
PRACTICAL APPROACH 7

- Share ORM self-assessment results with staff.
  - Benefits of include:
    - Set a positive organizational tone.
    - Foster greater awareness and deeply interesting to staff.
    - Involve entire team in management of operational risk.
    - Get everyone on the same page.

PRACTICAL APPROACH 7 (CONT.)

- Share ORM self-assessment results with staff.
  - Benefits of include:
    - May lead to identification of additional risks, scenarios, and potential management approaches.
    - Helpful from a developmental standpoint.

PRACTICAL APPROACH 8

- Use ORM self-assessment information to bring incoming managers up to speed:
  - Fantastic tool for quickly understanding current state and identifying desired changes.
  - Great way to learn about the operation and the staff.
  - Helpful in terms of accelerating the learning curve and minimizing surprises.
PRACTICAL APPROACH 8 (CONT.)

• Use ORM self-assessment information to bring incoming managers up to speed:
  – Good way to overcome discomfort without asking a lot of questions.
  – Preserves institutional knowledge and passes it along.
  – Sets an organizational tone of risk management effectiveness.

PRACTICAL APPROACH 9

• Make the operational risk management process a forum for constructive discussion of losses, near misses, and exposures:
  – Potential exists for great organizational learning.
  – Needs to be a safe environment.
  – Review incidents in which outcomes differed from expectations.

PRACTICAL APPROACH 9 (CONT.)

• Make the operational risk management process a forum for constructive discussion of losses, near misses, and exposures:
  – Use case study format.
  – Let the appropriate manager take the lead, with support from ORM.
PRACTICAL APPROACH 10

• Capture loss data where there is potential to add value:
  – Don’t do it just for the sake of doing it or because it’s what you’re supposed to do.
  – Have a vision for what will be done with the data and how it will improve organizational performance.
  – Partner with business leaders whose goals can be furthered through affiliation with ORM.

PRACTICAL APPROACH 10 (CONT.)

• Capture loss data where there is potential to add value:
  – Start with high-frequency low-severity losses like branch charge-offs.
  – There is value in putting a number on overall operational risk-related losses.

PRACTICAL APPROACH 11

• Monitor progress in the development and use of key risk indicators:
  – Lagging, leading, and concurrent indicators of changes in risk levels.
  – Significant activity trap potential.
  – Early progress in identifying top KRIIs for various businesses and functions.
PRACTICAL APPROACH 11 (CONT.)

• Monitor progress in the development and use of key risk indicators:
  – First benchmarking efforts underway.
  – Current efforts could result in development of helpful industry standard approaches.

PRACTICAL APPROACH 12

• Keep the program business-focused. Consider selecting an ORM leader or facilitator who comes from the business side of the institution:
  – Not an external hire (if possible).
  – Not a risk manager.
  – Not an auditor.
  – Need empathy for what life is like in a business role.

PRACTICAL APPROACH 13

• Pilot test any activity before unleashing it on the entire organization:
  – Look for volunteers from your advisory group.
  – Select people who will provide honest and thoughtful feedback.
  – Let participants know they are part of a pilot and ask them to be picky.
PRACTICAL APPROACH 13 (CONT.)

• Pilot test any activity before unleashing it on the entire organization:
  – Debrief participants at the conclusion of the activity.
  – Involve pilot participants in wider launch.

PRACTICAL APPROACH 14

• Collaborate with other support functions to ensure processes are effective and efficient:
  – Develop a clear vision as to how various functions fit together. Think of ORM as the umbrella that sits on top of various centers of expertise and more general business unit efforts.
  – Understand the perspectives of owners of related functions.

PRACTICAL APPROACH 14 (CONT.)

• Collaborate with other support functions to ensure processes are effective and efficient:
  – Get them on board with your vision before addressing specifics.
  – Demonstrate how the ORM program can help them be more effective and efficient.
PRACTICAL APPROACH 15

- Be judicious in your use of resources; stick to activities you believe in personally and for which you can articulate a clear value proposition:
  - Don’t build the ideal program; just the one that is ideal for your organization.
  - Don’t do anything just because others are doing it.

PRACTICAL APPROACH 15 (CONT.)

- Be judicious in your use of resources; stick to activities you believe in personally and for which you can articulate a clear value proposition:
  - Don’t do anything just because you think you are supposed to do it.
  - Don’t do anything just because regulators encourage it.

PRACTICAL APPROACH 16

- Participate in industry events to build networks, share ideas, and keep up with emerging approaches and best practices:
  - RMA’s Operational Risk Management Discussion Group is as good as it gets.
NEXT STEPS

• What approaches make the most sense for your organization?
• What do you intend to do differently when you get back to the office?

REVIEW OF MODULE 5 OBJECTIVES

• Consider practical approaches for a financial institution.
• Develop a course of action for when you return to the real world.

COURSE OBJECTIVES

• Define operational risk.
• Determine where operational risk fits relative to other risk types and why it is an increasing focus.
• Recognize the significance of the regulatory landscape.
COURSE OBJECTIVES

- Gain familiarity with tools and techniques used by operational risk practitioner.
- Consider practical approaches for managing operational risk in a financial institution.