Integrating IT Risk Management with ERM

Wednesday, June 18, 2014
7:30 AM to 9:00 AM

Vlad Liska, CIA, CISA, CRMA
Director, Operational Risk & Controls
TD Ameritrade
Learning Objectives

- Develop and implement an enterprise risk management framework
- Align the enterprise risk management framework to support the needs of IT
- Implement a multifaceted approach for embedding risk management activities into the everyday culture of IT
- Utilize tools and education to build support and drive adoption
- Foster a collaborative partnership between risk management and IT
Operational Risk
The risk of loss resulting from inadequate or failed processes, people and systems, or from external events.

Internal Failures or Breakdowns
- **People**: Failures of Employees, Management, Conflict of Interest, or Internal Fraud
- **Process**: Failures or Weaknesses in Key Processes, Non-Compliance with Policies, Regulations, or Failures in Products or Services
- **Technology**: Operational Failures, Code Defects, Security Vulnerabilities & Breaches

External Events
- **External**: Fraud or Litigation, Economic Conditions, Competitors, Political, Geographic
Types of Operational Risk

- Unauthorized Activity
- Reputational Risk
- Discrimination
- Human Error
- Product Liability
- Merger Risk
- Fraud
- Natural Disaster
- Advisory Risk
- Technology Failures
- Business Continuity
- Sexual Harassment
- Suitability
- Legal Risk
- Regulatory Risk
- Model Risk
- Data Security
- Project Management
- Operational Risk

Operational Risk
Specific Risk Types

- **Business Process Risk**
  - Transaction Processing Risk – Risk arising from failed internal processes related to the processing of transactions
  - Physical Security Risk – Risk arising from failed internal controls intended to protect physical assets
  - Business Continuity Risk – Risk resulting from business disruption

- **Technology Risk**
  - Risk associated with the use of systems and technology

- **Human Capital Risk**
  - Risk of loss arising from the actions and inactions of people

- **Compliance Risk**
  - Risk associated with compliance of laws, regulations, and policies

- **Legal Risk**
  - Risk associated with enforceability of contracts and interpretation of laws

- **Financial Risk**
  - Risk of loss arising from failed financial controls impacting the firm's ability to meet its operational and regulatory financial obligations

- **Vendor Risk**
  - Risk associated with the use of third party service providers for services or outsourcing of services

- **Implementation Risk**
  - Risk associated with operational and systems readiness to support and service products, systems, and clients
Evolution of Risk Management

- Additional Board Scrutiny During the Financial Crisis
- Evolution of the Chief Risk Officer Role
  - Importance of Governance, Risk, and Controls Framework (from Financial Crisis)
  - Risk Advocate with Executive Management Team
  - Clear Accountability for Risk Management Strategy and Execution
  - Set Tone from the Top about the Importance of being a Risk-Aware Organization
- Expanded Risk and Governance Structures
  - Board Risk Committee
  - Staffing Model for Risk Analysis
  - ‘Risk Appetite’ and Risk Management Frameworks
  - Tools to Support Risk Management
Roles, Responsibilities, and Tools

**Corporate Risk Governance**
- Develops, Maintains, and Enhances the Governance Structure
  - Report Generation & Data Sourcing
  - Maintain Charters, Minutes, and Policies
  - Tool & Application Development
  - Framework Development

**Corporate Risk Services (Insurance)**
- Impact Mitigation Utilizing Risk Transfer Techniques
  - Contract Review & Insurance Management
  - Claim Management & Coordination
  - Crisis Management

**Enterprise Continuity Management**
- Direction and Leadership in Preparing, Testing and Reporting on BCP; First Response for Business Interruption
  - Business Contingency Planning
  - Business Impact Analysis
  - Recovery Plan Testing
  - Continuity Event Management

**Internal Control Assessment Program (ICAP)**
- Assess Internal Controls are Operating as Designed
  - Quarterly Testing & Certification
  - Assessment of the Internal Controls (SOX)

**Corporate Risk and Controls (Risk Coverage Officers)**
- Promotes Adoption of a Consistent Framework in Organization
  - Point of Contact for Management
  - Implement Risk Framework
  - Risk Advisory
  - Risk Analysis
  - Assessment Activity
  - Exceptions and Risk Acceptances
  - Support Business Continuity
  - Proactive Risk Management

**Risk Management Tools**
- Utilize RSA Archer Platform (RSA GRC Modules)
  - Manage Risks, Demonstrate Compliance, and Automate Business Processes
  - Implemented Four Modules
    - Issue Management
    - Operational Risk Events
    - Key Risk Indicators
    - Strategic Risk Assessments

Corporate Risk Management (CRM) Mission Statement:
"Minimize unexpected losses/gains and earnings volatility, and provide management information that drives strategic decision making and helps the business meet its objectives"
Effective risk management requires managers to:
- Understand the actual and prospective risks facing their business and department
- Develop an opinion about, and define, their risk exposures
- Execute an effective strategy to mitigate controllable risks

Employees also need to:
- Recognize the risks in their business unit and its processes
- Know the actions they need to take to control those risks
Five Components of our ORM Framework

1. **Risk (Loss) Events**
   The collection and analysis of operational risk events (financial and non-financial), including the identification of the root cause that has led to their occurrence, the impact to the organization, and any remediation plans to mitigate such risk.

2. **Risk Indicators**
   The development of indicators and thresholds that management utilizes to effectively track and monitor changes in the levels of significant risk over a period of time.

3. **Risk Assessments**
   Management’s identification and assessment of its key risk areas and the effectiveness of related controls to mitigate such risk.

4. **Issue Management**
   The tracking and remediation of issues arising from risk management activities provides transparency to senior management and also enhances the ability of management to make decisions around potential mitigation strategies.

5. **Reporting, Analysis, & Governance**
   Deliver risk analysis and reporting to senior management which creates transparency and supports decision making.
1. Risk (Loss) Events

- Key Component for the Identification and Measurement of Operational Risk
  - Timely Notification and Comprehensive Reporting of Risk Events
- Risk Events occur when an Operational Risk Failure Takes Place and Leads to a Negative or Positive Monetary Impact, or Zero Impact with Potential Loss (Near Miss)
- Risk Management is Responsible for the Overall Risk Event Data Collection Process
  - Working with Management to Quantify Losses
  - Categorizing and Analyzing Data to Determine Systemic Issues to be Addressed and Lessons Learned (Root Cause Analysis)
- Management is Responsible for Ensuring that all Risk Events are Reported, Escalated, and Remediated as necessary

Financial Losses ($), CC Incident Materiality, Security Event Materiality, Policy Exceptions, Project Related, QA Defects, others?
2. Risk Indicators

- **Risk Appetite Metrics** are Board-level metrics that track risk to the maximum exposure the organization is currently prepared to accept for critical risk-producing activities.

- **Key Risk Indicators (KRIs)** are an indicator that management uses to effectively track and monitor changes in the levels of significant risk over a period of time.

- **Key Performance Indicators (KPIs) / Operating Metrics** are measurements used to gauge some quantifiable component of a department’s performance; used by department level management to monitor their day to day business activities.
2. Risk Indicators

Key Risk Indicators

- "Forward" Looking Measurements of Risk
- Relevant, Measurable, Predictive and Easy to Monitor
- By Themselves CANNOT Reduce Risks
- Escalation Thresholds as Trigger Points
- Trigger Mitigation & Response, Improve Communication & Transparency, Strengthen & Validate Risk Management
- Development: Key Processes, Key Risks, Existing / New Risk Indicators

![Diagram showing Key Risk Indicators]

- Engagement Survey
- Client Concentration
- Fail to Deliver / Receive ($)
- DR Readiness Index
- Incident Materiality
- Key Risk Indicators
- Ready Now Successors
- Emergency Change Frequency
- Client Complaints
- SARs Filled
- Voluntary Turnover
- Website Availability
- New Hire Training
- Third Party Claims

![Example KRI Graph]

Value: 1.6%

Reflects Monthly Reporting As of XXXXX/MMM

Example KRI

<table>
<thead>
<tr>
<th>Value</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1.6%</td>
</tr>
<tr>
<td>2</td>
<td>3%</td>
</tr>
<tr>
<td>3</td>
<td>7%</td>
</tr>
<tr>
<td>4</td>
<td>8%</td>
</tr>
</tbody>
</table>

12
3. Risk Assessments

- **Strategic Risk Assessments**
  Identify, evaluate and prioritize a group of business risks that could significantly impact a company’s or business unit’s ability to accomplish its business objectives

- **Internal Control Assessments**
  Ability for management to measure its system of internal controls

- **Product Risk Assessments**
  Applies to new products and/or services, new business initiatives, or existing products

- **Target Risk Assessments**
  Used to identify and measure the significance and likelihood of a control breach and possible financial or reputation impact that could occur within a function or specific process

- **Internal and External Audits or Examinations**
  Used to determine if there are systemic issues that need to be addressed, tracked, and remedied to completion

---

**Questionnaire / Assessment**
Evaluate on a scale of:

- **Low Risk**
- **High Risk**
  - Inherent Risk
  - Control Effectiveness / Risk Mitigation
  - Assess Residual Risk
4. Issue Management

- Issues are Raised in order for Management to Mitigate Risks of Future Losses or other Undesirable Events
- Issues are Documented and Tracked for Management to make Business Decisions on the Treatment of the Risk
- Identified Mitigating Plans need to be Tracked to Completion
- Issues from Various Sources Need to be Consolidated
5. Reporting, Analysis, & Governance

- Escalation, Reporting, and Monitoring of Operational Risk must be Sufficiently Transparent, Timely, and Actionable
- Risk Management is Responsible for Developing, Maintaining and Updating Standard Reporting Templates and Identifying and Managing Data Sources for Analysis
- Business Management is Responsible for Ensuring that Sufficient Information is Provided to all Levels of Management
- Control Groups are Responsible for Ensuring that Sufficient Reporting within their area of Expertise is Reported
KEY to SUCCESS: Executive management must set the tone on accountability and responsibility!
Proactive Risk Management

- **Proactive Engagement on Critical Projects and Initiatives**
  - **Enterprise Monitoring** – Maintain Awareness of Key Projects and Initiatives in the Organization
  - **Risk Assessment and Staffing** – Assess Projects and Initiatives by Risk in an Accurate and Timely Manner and Staff Appropriately
  - **Execution Framework** – Consistent Risk Checklist Approach
  - **Communication** – Raising Risks to Management

**Initiation**
- **Business Case** - Agreed-upon, detailed, realistic, measurable
- **Project Costs** - Clear estimates, agreement from stakeholders
- **Project Initiation** - Clear project sponsor, manager, methodology, repository, resources identified, approval

**Planning**
- **Privacy** - Protection of information, authorization, approval, use, storage, third party access, destruction
- **Vendor Management** - Relationships, single points of failure, outsourcing, data and system access, contract sufficiency
- **Brand / Reputation** - Protection and processes

**Execution**
- **Human Capital** - Management and staff adequacy, key personnel reliance, employment practices, workplace safety
- **Procedures** - Process, SLA’s, helpdesk, application support, programming documentation, helpdesk procedures, data center procedures
- **Communication** - Completion, approval, meetings

**Post-Implementation**
- **Post-Implementation** - Project closure, monitoring, follow-up, lessons learned
- **Open Defects** - Closure status, reassignment of open items
Conclusion

➢ Risk Management is a Journey, not a Destination

➢ More to Come…

Thank You!