A Guide to IT Risk Assessment for Financial Institutions

March 2, 2011

Pivot Group and Porter Keadle Moore present:

*Webinar Series: Enterprise Risk Management for Financial Institutions*
Welcome!

Housekeeping...

- Control panel on the right side of your screen.
- Audio
  - Telephone
  - VoIP
- Submit “Questions” in the pane on the control panel and we will address questions at the end of the session.
- Minimize pane during presentation – Click double arrows icon top-left of the control panel.
- Need help? Call 800-263-6317
**Introductions**

**Presenters:**

- **Jim Soenksen**, CEO, Pivot Group, LLC
- **Chris Bowler**, Senior Manager, Porter Keadle Moore, LLP
Introductions

- **Pivot Group**
  Independent Audit, Assessment and Compliance Firm providing exclusively Data Privacy and Protection Services

- **Porter Keadle Moore**
  A leading Atlanta accounting firm offering a full range of assurance and advisory services in the areas of audit, tax and systems.
February 16  - Building an Enterprise Risk Management Program

Today  - A Guide to IT Risk Assessment

March 16 – Identifying and Classifying Critical Data Risks

March 30 – Applying Risk Assessment Activities to your Business Processes-Lending

April 13  - Enterprise Risk Management Programs: Pulling the Pieces Together
Today’s Learning Objectives

- What should be included in an IT Risk Assessment
- How it fits into the ERM Framework
- Share effective audit techniques and tools
- Who needs to be involved in the process.
- The ideal timing to perform your assessment
Today’s Agenda

- Review of Session One Main Points
- How to Assess Your IT Operation’s Strategic, Financial, Operational and Compliance Risks
- Case Study
- Recommended Audit Techniques
- Audit Tools that Can Help
- Risk Mitigation Best Practices
- Questions
Review: Building Your ERM Check List

- Identify & Tailor Your Framework
- Establish a Communication Plan
- Confirm Business Goals & Objectives
- Identify Key Business Processes & Owners
- Define Risk Context & Terms
- Complete Baseline Risk Assessment
- Agree to Residual Risks & Responses
- Create Monitoring Mechanisms
- Begin Reporting Cycle
Review: Elements of An Effective Risk Management Program

- Establish Risk Context
- Risk Identification
- Risk Analysis
- Risk Evaluation
- Risk Response

Based on ISO 31000
Effective Risk Management Program

- Includes a systematic top-down approach;
- Summarizes the risks associated with the key business units and/or processes.
- Provides a common view that ranks risks and the risk management activities.
- Is based on information, analysis and process understanding.
- Assists management with establishing a baseline risk profile.
Objectives for Information Systems

- Completeness and Accuracy of Transaction Processing
- Restricted Access to Programs & Data
- Accurate and Complete Customer Information
- Timely Access to Management Reporting
Key Risks

Objectives

Relevant Risks

Strategic
- Reputation
- Customer Changes
- Product/Services Management & Development
- Competition

Operational
- Qualified Personnel
- Transaction processing
- Access to information
- Vendor management
- Information disclosure
Risk Ratings

- **Low**: Risk is less than remote with minimal impact on business performance
- **Medium – Low**: Risk is remote with some minor (< 5%) impact on business performance
- **Medium**: Risk is possible with moderate impact (5% - 10%) on business performance
- **Medium-High**: Risk is present with significant impact (10% - 20%) on business performance
- **High**: Risk is present with material impact (>20%) on the business performance
Review: Defining Your Risk Appetite & Profile

Objectives

Relevant Risks

Management Experience
Practices
People
Systems
Risk Management Maturity Model

- **Ad-Hoc**: There are not any organizational wide established basic risk management processes; however, some established business units and areas have risk management processes, but these are applied only on an ad-hoc and sporadic basis to various business processes.

- **Basic**: Some basic risk management processes and standards have been established within the organization, but are required only on selected complex, critical, or high-visibility business processes with certain dollar thresholds, or with certain customers.
Risk Management Maturity Model

- **Structured**: Risk management processes and standards are fully established, institutionalized, and mandated throughout the entire organization.

- **Integrated**: Basic risk management processes are integrated with other organizational core processes such as cost control, schedule management, performance management, and systems engineering.

- **Optimized**: Risk management processes are evaluated periodically using efficiency and effectiveness metrics. Continuous process improvement efforts are implemented to improve the risk management processes across all business units.
Considering Changes

- **External**
  - Economic
  - Market
  - Competitors
  - Regulatory

- **Internal**
  - Organizational
  - Practices
  - People
  - Systems
"If you're in a bad situation, don't worry it'll change... If you're in a good situation, don't worry it'll change. “ John A. Simone, Sr.
Complexity!

Some Indicators:
- Centralized vs. Decentralized;
- Management of Internal and External Resources;
- Level of Integration For System Interfaces;
- Manual vs. Automated; and
- Cross-Functional Teams;
How to Assess Your IT Operation:
IT Areas Included

- Based on the results of your ERM Phase 1….
- Organization Structure including roles and responsibilities
- Policy and Procedures
- Configuration and Change Management Activities
- Information Security Architecture
- Information Security Administration
- Current and Future Software Applications
- Records Management and Data Classification
- Culture and Awareness
How to Assess Your IT Operation: IT Areas Included-Continued

- Access Controls
- Data Center Operation
- End User Support Activities
- Data and Network Security Controls
- Availability of Data for Financial and Managerial Reporting
- Business Continuity and Disaster Recovery Plans
- Physical Controls
How to Assess Your IT Operation: Approach

- **Survey Inherent Risks**
  - Include Internal and External Risks
  - Identify the Degree and Sources of Risks
  - Review complexity of Key IT Support Functions
  - Determine indicators of increasing and decreasing risks

- **Review Specific Risk Response Activities**
  - Assess strength of IT Control Environment
  - Review Policy and Procedures
  - Assess the information supporting management’s decisions
  - Review the nature and timing of control activities
Determine Residual Risks

- Identify key risk & performance indicators
- Evaluate the probability and severity
- Assess current risk mitigation activities
- Provide risk management improvement recommendations
Case Study - Objectives

- Qualitative IT Risk Assessment
- Identify Inherent **Strategic** and **Operational** Risks
- Considers Control Activities
- Identifies Resources In Place
- Evaluate Risk Management Process Change Capabilities
- Area of Focus: Information Security-Logical Access to Programs and Data
- Vendor Management
Case Study - Relevant Risks

- Unauthorized disclosure of PII
- Data Integrity/System Vulnerabilities
- Operational Interruption/System Availability
Case Study: Operational Risk

Definition: Tangible Internal Risks related to:

- Internal controls
- Operating Processes
- Management Information Systems
- Employee/Vendor Integrity
Case Study: Residual Operational Risks

- Policies and Procedures Out of Date
- Network/systems Managed Internally
- Good Layered Network Defenses
- User Access Granted by Authorized Management
- Informal User Termination Process
- Change Management Activities not Documented
- Security Logs not Proactively Reviewed
- Network Access Authentication Exists
Network Level Access does not enforce segregation of duties
Network Administration Activities are not consistently documented or reviewed
Outside Vendor performs PCI Scanning
Vendor Management Program does not exist
Physical Access Controls are good
External Annual Audit performed; No material deficiencies
Case Study: Residual Strategic Risks

- **Reputation:** Unauthorized Exposure of PII based on operational risk.
- **Security Architecture:** The overall architecture is good. Deficiency in monitoring, alerting, governance, and oversight.
**Case Study: Risk Rating**

- Inherent Risks: Medium High
- Residual Operational Risks: Medium
- Residual Strategic Risks: Medium Low

<table>
<thead>
<tr>
<th>Process Area: Information Security - Logical Access to Programs &amp; Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quality of Management Activities</td>
</tr>
<tr>
<td>-----------------------------------</td>
</tr>
<tr>
<td>Basic ●</td>
</tr>
</tbody>
</table>
Stakeholders For Your ERM

- CEO
- CFO
- COO
- CIO
- Chief Risk Officer
- Chief Compliance Officer
- Data Privacy Officers
- Audit- Internal/External
- Business Unit/Department Owners
Information Collection Techniques

- Interviews and Group Discussions
- Check Lists, Questionnaires, and Surveys
- Documentation Reviews
- Test Sampling Examples
  - Data Discovery
  - Walk-A-Rounds
  - Management Reports
  - Incident Reports
  - Personnel Files
  - Policy and Procedures
  - IT Systems Controls
Tools That Can Help

- Survey and Questionnaire Software
- Remote Meeting Software
- Document Sharing/Share Point
- Remediation Tracking
- Data Discovery
- Evaluation and Scoring Metrics
- Risk Management Dashboard
- Governance, Risk, and Compliance Software
Risk Mitigation Best Practices

- Formal Information Security Program
- Implementation of Policy, IT, and Awareness Controls
- Regular Reviews of Policies and Procedures
- Current Awareness and Training Programs
- Regular Tests of Security Controls
- Regular Tests of IT Controls
- Regular Critical Vendor Reviews
- Regular Review of Incident Response Program
- Regular Review of BC/DR Program
Risk Mitigation Best Practices - Continued

- Regular Data Discovery and Inventory
- Regular Review of Records Management Program
- Establish a Baseline
- Continual Improvement of Baseline
- Establish a Risk Management Committee
IT Risk Assessment Best Practices: When to Perform

- Perform at least annually
- Perform when a significant event is about to occur
- Perform when a significant event has occurred
- Utilize objective resources
- Research and Confirm regulatory compliance obligations
- Validate Critical Data Location and Controls
- Continual Remediation, Validation, and Monitoring
IT Risk Assessment Check List

- Base IT Assessment on ERM Framework
- Establish a Risk Management Committee
- Determine Objectives
- Identify Relevant Risks
- Determine Scope
- Include *all* Internal Stakeholders
- Identify *all* Critical External Parties
- Determine Best Information Gathering Techniques
- Perform Objectively
- Agree on Mitigation Best Practices
- Establish Risk Baseline
- Build on Continual Improvement
Next Webinar

- **March 16** - Identifying and Classifying Critical Data Risks

Learning Objectives

- Techniques for Identifying and Classifying Critical Data
- Compliance Requirements for Data and Personal Identifiable Information (PII)
- Data Protection Best Practices
- Examples of Technologies that Can Help
- A “Checklist” of Critical Success Factors for Data Risk Management
Questions?
Contact Information

Jim Soenksen – Pivot Group
- jsoenksen@pivotgroup.com
- 888-722-9010
- www.pivotgroup.com

Chris Bowler- PKM
- cbowler@pkm.com
- 404-420-5929
- www.pkm.com