Risk Management and Internal Audit Specialized Training Course

Audit Risk Assessment Methodology

May 20, 2015
TO KNOW WHAT LIFE IS WORTH YOU HAVE TO RISK IT ONCE IN A WHILE.

JEAN-PAUL SARTRE
Risk and Risk Assessment Defined

Risk
Institute of Internal Auditors (IIA)
The probability that an event or action may have an adverse affect on the organization or activity under audit

Committee of Sponsoring Organizations (COSO)
Threats to a business entity achieving its objectives, mitigated by appropriate controls

Risk Assessment
Institute of Internal Auditors (IIA) Definition
A systematic process for assessing and integrating professional judgments about probable adverse conditions and/or events .... [a means to] develop the audit work schedule
Risk Assessment

Federal Reserve System

- The risk assessment measures relative risk in Bank operations which enables appropriate audit coverage using a risk-based approach
  - Structured, objective, quantifiable and defensible
  - Affords flexibility and professional judgment
  - Easy to use and understand
  - Universally applicable

- The Fed’s RAM is regularly reviewed to ensure we keep current with industry practices. Focus includes:
  - Focus on inherent risk
  - Emphasis on human resource risk
  - Emphasis on change and complexity (Emerging Risks)
Risk Assessment Process

- Identify audit universe and auditable activities
- Apply risk model
- Annual risk assessment and ranking
- Annual Audit Program based on:
  - risk ranking
  - frequency guidelines
  - professional judgment
Risk Model

Risk Assessment including Scoring Matrix

- Gathering of information and assessment of risk
- Enables auditable activities to be ranked for the purpose of scheduling audit coverage
Risk Assessment

- Documents the risks related to an auditable entity in the audit universe.
- Can be utilized in developing audit scope.
- Information sources include:
  - Audit management
  - Bank management
  - Recent audit coverage
  - Operational risk management program
  - Irregular occurrences
  - Audit liaison relationship with client
Risk Factors

Operational
- Business Process
- Technology and Information Management
- Human Resources

Financial/Materiality (includes Credit Risk and Market Risk)

Strategic

Reputational
Operational Risk

- The risk of **direct or indirect loss** or other negative effects to a Federal Reserve entity as the result of inadequate, ineffective, or **failed internal processes**, people, or systems, or from **external events** that impair those internal processes, people, or systems.

- **Examples:**
  - Management does not confirm that vendors do not meet performance thresholds as stated in the contract and as a result penalties are not assessed.
  - Users are not recertified for the Bank’s major systems on a stated frequency to ensure users’ access is appropriate.
Financial Risk (includes Credit Risk and Market Risk)

Financial

- The risk of the **financial materiality** in a given business process and its potential impact on the Bank or the System. The probability that the Bank will suffer a loss because a **counterparty cannot meet its financial obligations** (Credit Risk). The probability of **adverse movements in market rates** (Market Risk).

- **Examples:**
  - Borrower or counterparty fails to meet its obligations in accordance with agreed terms.
  - Currency devaluations are not monitored timely which may impact borrowers’ ability to borrow from the Discount Window.
Strategic Risk

- The risk that the Federal Reserve entity will not achieve its mission or objectives because its strategic planning process, leadership, or implementation of its strategic plan is not fully effective.

Examples
- The Markets team mission and strategic objectives do not exist and/or do not align to the Bank’s overall mission and strategic objectives.
- A succession planning model is not developed for senior management which may cause an environment of fear and uncertainty.
Reputational Risk

- The risk that a Federal Reserve entity will fail to comply with applicable laws or manage risks, or that external events or a lack of the fulfillment of the Federal Reserve’s role, either real or perceived, could diminish the Federal Reserve’s stature.

Examples:
- Negative press from the WSJ or NY Times may impact the Bank’s reputation and may turn away potential borrowers.
- Confidential information is leaked which may damage the Bank’s credibility.
Scoring the Risk Factors

- Each Risk Factor is assigned a rating, or risk level:
  4: High
  3: Moderately High
  2: Moderate
  1: Low
Inherent vs. Net Risk

Inherent Risk

- measures variability prior to the application of controls.
- can be evaluated by taking into account impact and likelihood.
- change and complexity increase this risk.

Residual Risk (Net Risk)

- Inherent risk not mitigated by the control environment is considered residual (net) risk.
- Audit tests the control environment and opines on the level of residual risk.

Control Environment

- the collective actions taken by business management to eliminate or reduce inherent risk.
- full risk mitigation is not necessarily the objective.
Mitigating Control Factors

Strong internal controls help mitigate some of the risk factors and lower the overall risk of the business unit.

Mitigating factors may include but are not limited to

- External Reviews
- Internal Audits
- Performance Measures
- Indicating Quality Control Activities
- Effective Staff Training
- Experienced Management
- Experienced Staff
- Monitoring Activities
- Management Self Risk Assessment
Scoring Process

- Factor Weights (Pre-determined)
- Factors assigned Risk Levels 1 through 4
- Factor Scores (Weight x Risk Level)
- Overall Score (Sum of Factor Scores)
## Audit Frequency

<table>
<thead>
<tr>
<th>Risk Rating</th>
<th>Score Range</th>
<th>Maximum Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>326 - 400</td>
<td>Each calendar year</td>
</tr>
<tr>
<td>Moderate</td>
<td>251 - 325</td>
<td>Within 3 years</td>
</tr>
<tr>
<td>Low</td>
<td>100 - 250</td>
<td>General Auditor discretion</td>
</tr>
</tbody>
</table>

**Note:** High risk audits can be extended to two years based on influencing factors
Completing the Scoring Matrix

Inherent Risk Rating
- High, Moderate or Low

Mitigating Factors
- schedule neutral
- increase audit frequency
- decrease audit frequency

Recommended Schedule
- immediate
- annual
- within two years
- within three years
- other
Influencing Factors

- Account for specific processes or functions that the auditor believes pose high or moderately high risk.

- Noted separately to allow for additional dialogue and consideration about audit scheduling.

- These processes or functions may warrant:
  - review on a greater frequency than the business area as a whole
  - separate or centralized audit coverage
# Risk Assessment Scoring Matrix – Excerpt from AA

## Risk Assessment Scoring Matrix

<table>
<thead>
<tr>
<th>RISK FACTOR</th>
<th>WEIGHT</th>
<th>RISK LEVEL (H=4, M=3, L=1)</th>
<th>SCORE (wgt. x level)</th>
<th>PRIOR SCORE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operational</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Business Processes</td>
<td>20</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2. Technology and Information Management</td>
<td>20</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3. Human Resources</td>
<td>20</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Financial/Materiality</td>
<td>20</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Strategic</td>
<td>10</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Reputational</td>
<td>10</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td>100</td>
<td></td>
<td></td>
<td>0</td>
</tr>
</tbody>
</table>

**Inherent Risk Score Frequency:**

**Influencing Factors:**

**Recommended Frequency:**

<table>
<thead>
<tr>
<th>Risk Rating</th>
<th>Inherent Risk Score</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>326 - 400</td>
<td>Each calendar year but can be extended to two based on influencing factors</td>
</tr>
<tr>
<td>Moderate</td>
<td>251 - 325</td>
<td>Every three calendar years</td>
</tr>
<tr>
<td>Low</td>
<td>100 - 250</td>
<td>General Auditor discretion</td>
</tr>
</tbody>
</table>

**Other Audit Schedule Considerations:** Please identify those areas within the scope of this business profile that represent high or moderately-high risk. Identification of these processes or sub-functions may facilitate the audit planning step or they may be used to determine areas that are included in another audit that more directly addresses the risk. For example, if the business area's IT functions are complex and represent high risk, these IT functions may merit review on a greater frequency than the business area as a whole. In this example, one solution may be to include these IT functions as part of an audit that focuses on IT type audit.
Risk Assessment – Excerpt from MKi
Annual Audit Plan

- Higher audit priorities are generally assigned to activities with higher risk (e.g. WPO, OEB, SOMA, etc.)

- The **timing** of audit attention is flexible within the Annual Audit Plan

- The Risk Assessments which include risk rankings and the Audit Plan are reviewed and modified at least annually

- Individual risk factor ratings are considered when planning the scopes of individual audits
The RAM is defined within the context of the IIA Standards
The RAM applies to all business activities in the Federal Reserve System
Risk assessments is based on inherent risk
The overall risk assessment process has four steps:
- identification of the auditable activities in the universe
- documenting risk assessment and scoring
- ranking of activities according to risk
- scheduling of audit coverage based on the risk assessment
Influencing factors should be considered which can affect audit frequency
Useful Links and References for Risk Assessments

- http://www.ey.com/Publication/vwLUAssets/EY_Key_considerations_for_your_internal_audit_plan_1/$FILE/ATT5QP7A.pdf

Applicable IIA Standards

- **Standard 2000** – Managing the Internal Audit Activity
- **Standard 2010** – Planning
- **Standard 2200** – Engagement Planning
Questions