Risk Assessment and Risk Acceptance Overview

Presented by: Bernice Lemaire, CPA, CIA, CGFM, CGMA, CFE
Office of Benefits Administration (OBA)
Manager, Management Compliance Division, OBA Chief Auditor and Member PBGC Risk Management Council

November 8, 2016
Objective

• Provide a tactical approach to risk assessment and risk acceptance determination and reporting
Definition – Residual Risk

• OMB A-123
  – Residual Risk - Residual risk is the exposure remaining from an inherent risk after action has been taken to manage it, using the same assessment standards as the inherent assessment

• COSO ERM Framework Revision Exposure Draft (June 2016)
  – Residual Risk - is the risk remaining after management has taken action to alter its severity.
Definition – Risk Acceptance

• OMB A-123 Definition
  – Risk Acceptance - No action is taken to respond to the risk based on the insignificance of the risk; or the risk is knowingly assumed to seize an opportunity.

• COSO ERM Framework Revision Draft Definition
  – Risk Acceptance - No action is taken to affect the severity of the risk. This response is appropriate when the risk is already within risk appetite. A risk that is outside the entity’s risk appetite and that management seeks to accept will generally require approval from the board or other oversight bodies.
What is COSO?

- The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a joint initiative of the five private sector organizations and is dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management, internal control and fraud deterrence.
PBGC’s Office of Benefit Administration’s Operational Risk Assessment

• Objectives:
  – To enhance governance and oversight
  – To plan and prioritize MCD review and compliance work more effectively and efficiently using a risk based approach
  – Apply Management Oversight and MCD review and compliance resources where they will have the most bang for the buck
  – Inform the FMFIA attestation process
  – Respond to OIG recommendation
OIG Recommendations

• Develop and document a risk assessment of the BAPD’s entire operations. The risk assessment should include the identification of root causes of the issues identified by the auditors and ASD. PBGC should monitor the implemented corrective actions. The materiality threshold used should be reasonable. (OIG Control #FS-14-04)
  — Closed 10/2016

OBA Approach to Risk Management

- Identify Scope (Business Process Universe)
- Develop Criteria Magnitude and Vulnerability Attributes
- Perform Risk Assessment
- Develop MCD Strategic Plan

- Magnitude Attributes
- Risk Assessment (by process)
- MCD Strategic Plan
- Individual Review/Compliance and Special Project Plans

- Vulnerability Attributes

- OBA FMFIA Management Assertion Process
- OBA Risk Management Program Statusing and Monitoring
- Supplemental SWOT Analyses

- Heat Maps/Dashboards
- Periodic Executive Risk Owner Reports
Develop Your Assessment Criteria

- Magnitude/Impact/Severity
- Likelihood/Vulnerability
<table>
<thead>
<tr>
<th>Criteria</th>
<th>Financial Statement</th>
<th>Reputation</th>
<th>Legal/Regulatory</th>
<th>Customer</th>
<th>Employees</th>
<th>Other</th>
<th>Stakeholder</th>
</tr>
</thead>
<tbody>
<tr>
<td>RATING</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VERY HIGH (5)</td>
<td>&gt;$34.1M*</td>
<td>Sustained U.S. national (and international) negative media coverage (front page of paper or business section)</td>
<td>Major federal or state action/Fraud or bribery or other legal investigation/action</td>
<td>Major loss of customer satisfaction</td>
<td>Significant/Uncontrolled attrition, flight from PBGC due to lack of confidence in long-term business or management capabilities. Includes significant workplace safety issues, morale issues and ethics/integrity issues.</td>
<td>Major modification to strategy</td>
<td>Catastrophic impact on performance, such as major IT system failure/breaching/sabotage OR PBGC cannot pay benefits.</td>
</tr>
<tr>
<td>HIGH (4)</td>
<td>$20M-$34.1M</td>
<td>Negative U.S. national or international media coverage (not front page)</td>
<td>Federal or state investigations or action</td>
<td>Degradation of relationship with customers and severe customer satisfaction rating drop</td>
<td>Frequent/significant workplace issues such as workplace safety and morale issues, stagnation and lack of growth opportunities</td>
<td>Modification to strategy</td>
<td>Severe impact on the business units operational performance OR large number of benefit payments cannot be made.</td>
</tr>
<tr>
<td>MEDIUM (3)</td>
<td>$5M-$20M</td>
<td>Negative media coverage in specific U.S. region or a foreign country, large plan involvement, many customers involved.</td>
<td>Few Federal or state investigations or action, routine costly litigation</td>
<td>Frequent, significant instances or sustained quality issues/conflict with customer(s)</td>
<td>Morale or satisfaction or commitment issues including salary OR benefits dissatisfaction.</td>
<td>Isolated modification to strategy as it relates to particular goals and customer service</td>
<td>Some damage requiring management attention. Minor system failure OR Benefit payments cannot be made to beneficiaries of certain plans.</td>
</tr>
<tr>
<td>LOW (2)</td>
<td>$1M-$5M</td>
<td>Localized negative impact on reputation (such as a small plan/ several customers involved) but recoverable</td>
<td>Smaller regulatory, legal actions, or penalties/fines</td>
<td>Occasional negative issues/feed back from customer(s) not easily resolved</td>
<td>Career progression, salary issues, work-life balance issues</td>
<td>Isolated modification to strategy as it relates to BAPD and/or minor outcomes/services.</td>
<td>Noticeable, but limited impact on operations OR benefit payments cannot be made to individual beneficiaries.</td>
</tr>
<tr>
<td>VERY LOW (1)</td>
<td>&lt;$1M</td>
<td>No press exposure</td>
<td>No regulatory or legal action</td>
<td>Infrequent issues/conflict with customer(s), easily resolved</td>
<td>Occasional employee issues, easily resolved</td>
<td>Course corrections easily achieved through normal business practices.</td>
<td>No loss of operational capability OR no impact on PBGC's ability to pay benefits.</td>
</tr>
</tbody>
</table>

*This is the 2014 Management Letter materiality threshold for the single employer program as determined by PBGC's Financial Operations Dept.
### Vulnerability Factors

<table>
<thead>
<tr>
<th>RATING</th>
<th>Controls/ Mitigation</th>
<th>Monitoring/ Testing/Reporting</th>
<th>Previous Risk Experience</th>
<th>CAPABILITY</th>
<th>Systems/Data/Security/ Technology</th>
<th>Expansion or Contraction (business, people, process, systems)</th>
</tr>
</thead>
<tbody>
<tr>
<td>VERY HIGH (5)</td>
<td>Controls are ineffective or do not exist</td>
<td>No controls monitoring, testing &amp; reporting</td>
<td>500K or other moderate recent previous adverse experience, e.g. significant deficiencies/audit findings</td>
<td>Minor knowledge/influence over third parties and/or third party relationships are volatile.</td>
<td>Risk affects a non critical process OR number of processes OR is a complex process; Process is somewhat immature, with significant variability in execution/outcomes.</td>
<td>Risk is managed by or directly impacts people, processes, systems or divisions that have experienced a significant rate of change over the last 6 months</td>
</tr>
<tr>
<td>HIGH (4)</td>
<td>Controls are somewhat effective. Can detect some risk.</td>
<td>Sufficient monitoring, testing &amp; reporting</td>
<td>Minor recent previous adverse experience, e.g. a reportable condition or finding</td>
<td>Sufficient knowledge/influence over third parties and/or relationships have occasional issues.</td>
<td>Risk affects a non critical process OR number of processes OR is a simple process; Process is significantly mature, predominately systematic with limited variability in execution and outcomes.</td>
<td>Risk is managed by or directly impacts people, processes, systems or divisions that have experienced a moderate rate of change over the last 6 months</td>
</tr>
<tr>
<td>MEDIUM (3)</td>
<td>Controls detect &amp; prevent risk</td>
<td>Extensive monitoring, testing &amp; reporting</td>
<td>No recent previous adverse experience</td>
<td>Very sufficient knowledge/influence over third parties and/or third party relationship issues.</td>
<td>Risk affects a non critical process OR number of processes OR is a simple process; Process is quite mature, systematic, little/no variability in execution or outcomes, repeatable, sustainable.</td>
<td>Risk is managed by or directly impacts people, processes, systems or businesses that have experienced a minor rate of change over the last 6 months</td>
</tr>
<tr>
<td>LOW (2)</td>
<td>Controls are very effective at detecting &amp; preventing risk</td>
<td>Extensive monitoring, testing &amp; reporting</td>
<td>No recent previous adverse experience</td>
<td>Very sufficient knowledge/influence over third parties and/or third party relationship issues.</td>
<td>Risk affects a non critical process OR number of processes OR is a simple process; Process is quite mature, systematic, little/no variability in execution or outcomes, repeatable, sustainable.</td>
<td>Risk is managed by or directly impacts people, processes, systems or businesses that have experienced no rate of change over the last 6 months</td>
</tr>
<tr>
<td>VERY LOW (1)</td>
<td>Controls are very effective at detecting &amp; preventing risk</td>
<td>Extensive monitoring, testing &amp; reporting</td>
<td>No recent previous adverse experience</td>
<td>Very sufficient knowledge/influence over third parties and/or third party relationship issues.</td>
<td>Risk affects a non critical process OR number of processes OR is a simple process; Process is quite mature, systematic, little/no variability in execution or outcomes, repeatable, sustainable.</td>
<td>Risk is managed by or directly impacts people, processes, systems or businesses that have experienced no rate of change over the last 6 months</td>
</tr>
</tbody>
</table>
Engage Assessors

- Offer and hold multiple sessions for risk assessors to obtain feedback on assessment criteria, finalize assessment criteria and to train them on how to use the assessment criteria
- Ensure that assessment teams are made up of process Subject Matter Experts and process Stakeholders
Document Assessment Results

• Important document assessment session results
  – You will need the information to put together relevant response plans

• Keep it simple use a Word document if you don’t have a fancy smancy system
Risk Profile
Budget - Execution

Strategic Objective(s):
Maintain high standards of stewardship and accountability; Pay pension benefits on time and accurately; Preserve plans and protect pensioners.

Mega Process: Operating Plan Development - Budgeting
Source: Management Input

Executive Risk Owner (ERO): Laura Smith (as of 02/19/2016)
Subject Matter Experts Consulted: Craig C., Deborah H., Andrea S., Kenra H.

Sub Process: Budget Execution

Risk Description: BAPD’s goals and objectives may not be met if status of funds are not monitored and funds are not made available and used according to plan.

Identify Contributing Risk Factors (internal or external)

- Funding may not be available to respond timely to changes in priorities if status of funds reports are not reliable/complete. As a result, off-cycle requests may be required.
- There may be an unwavering determination to spend funds the way they were initially planned.
- An emphasis may be placed on funding/accomplishing daily tasks without considering the impact on the strategic goals.
- The results of expenditure monitoring, such as status of funds reporting, may not be analyzed to determine expenditure’s effectiveness.
- Funds which are limited may be improperly allocated to lower priority projects.
- Monitoring and reviewing fund usage may not occur to ensure that funds are expended as planned.
- Monitoring (testing) by BAPD of processes, controls and risk related to budget execution may be minimal.
- The availability of funds may be subject to continuing resolutions issues.

Identify Risk Interrelationships and Interdependencies

- The CFS System
- Comprizon Suite -- acquisition management application

References:
- FM 10-1 PBGC Budget Preparation and Execution Process
- (OMB) Circular No. A-11: Preparation, Submission and Execution of the Budget
- Appropriation Law: Purpose and Use Statute
- FM15-02 Obligating Procedures for PBGC Procurements

Prepared by: Cate H. Date: 2/19/2016
Reviewed by: Bernice Lemaire Date: 02/21/2016
# Risk Profile - Mega Process Name
## Budget - Execution

<table>
<thead>
<tr>
<th>Assess Gross Risk Magnitude</th>
<th>Rate Scale: VH=5, H=4, M=3, L=2, VL=1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial Est Impact to Financial Statements</td>
<td>Overall Magnitude Rating: 1.13 Very low</td>
</tr>
<tr>
<td>Reputation</td>
<td>Legal/Regulatory</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Assess Vulnerability</th>
<th>Rating Scale: VH=5, H=4, M=3, L=2, VL=1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability Factors</td>
<td>Rating</td>
</tr>
<tr>
<td>Controls / Risk Mitigation Measures:</td>
<td>1</td>
</tr>
<tr>
<td>• Multiple people review requisitions before they are finalized</td>
<td></td>
</tr>
<tr>
<td>Controls Monitoring, Testing and Reporting:</td>
<td>1</td>
</tr>
<tr>
<td>• Very low risk because the movement of money for requisitions is very slow, so there is plenty of time to review and make corrections</td>
<td></td>
</tr>
<tr>
<td>Previous Risk Experience:</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Training, Resources, Skills and Knowledge:</td>
<td>2</td>
</tr>
<tr>
<td>• Staff in charge of Budget Execution is very knowledgeable in the subject</td>
<td></td>
</tr>
<tr>
<td>• Would benefit from additional staff knowing the process</td>
<td></td>
</tr>
<tr>
<td>Other:</td>
<td></td>
</tr>
</tbody>
</table>

---

2
Develop Useful Dashboards and Status Reporting Methods
# Excel Dashboard with Conditional Formatting

<table>
<thead>
<tr>
<th>Process Name</th>
<th>Sub Process Name</th>
<th>Significance</th>
<th>Magnitude</th>
<th>Vulnerability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appeals Correspondence</td>
<td></td>
<td>5.12</td>
<td></td>
<td>2.06</td>
</tr>
<tr>
<td>Benefits Adjustments</td>
<td></td>
<td>1.25</td>
<td></td>
<td>1.75</td>
</tr>
<tr>
<td>Benefit Calculations</td>
<td></td>
<td>2.00</td>
<td></td>
<td>1.16</td>
</tr>
<tr>
<td>Benefits Determination</td>
<td></td>
<td>3.00</td>
<td></td>
<td>1.00</td>
</tr>
<tr>
<td>Benefits Determination Letters</td>
<td></td>
<td>0.00</td>
<td></td>
<td>3.00</td>
</tr>
<tr>
<td>Benefits Determination Letters</td>
<td></td>
<td>10.43</td>
<td></td>
<td>5.83</td>
</tr>
<tr>
<td>Benefits Determination Letters</td>
<td></td>
<td>7.52</td>
<td></td>
<td>2.75</td>
</tr>
<tr>
<td>Benefits Determination Letters</td>
<td></td>
<td>1.00</td>
<td></td>
<td>1.00</td>
</tr>
<tr>
<td>Benefits Determination Letters</td>
<td></td>
<td>1.00</td>
<td></td>
<td>1.00</td>
</tr>
<tr>
<td>Benefits Determination Letters</td>
<td></td>
<td>4.22</td>
<td></td>
<td>3.38</td>
</tr>
<tr>
<td>Benefits Determination Letters</td>
<td></td>
<td>1.00</td>
<td></td>
<td>1.00</td>
</tr>
</tbody>
</table>

*Note: Magnitude and Vulnerability values are based on a scale of 1 to 5.*
OBA Quarterly Risk Management Status Report
Executive Risk Owner
Andrea S.
October 4, 2016

Appeals Correspondence
This OBA Quarterly Risk Management Report has been reviewed and accepted by the Chief Office of Benefits Administration.

__________________________________                  Date: ______________________

Cathy Kronopolus, CBA

CBA Comments (optional):
OBA Wide Process Heat Map
Mega-processes and Sub-processes

Key:
(1) Process Name
(2) Process Name etc.
### Office of Benefits Administration, Risk Summary as of 10/4/2016

<table>
<thead>
<tr>
<th>#</th>
<th>Process Risk Name</th>
<th>Quarterly Rankings</th>
<th>Executive Risk Owner</th>
<th>Upcoming Risk Management Milestone</th>
<th>Risk Management Summary Schedule</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Appeals Correspondence</td>
<td>Q2: High, Q3: High, Q4: High, Current: High</td>
<td>Andrea S.</td>
<td>Quarterly escalation report of appeals correspondence</td>
<td>Quarter end, beginning first quarter in FY 2017</td>
</tr>
</tbody>
</table>

**Legend:**

**Residual Risk -** Considering risk responses and the remaining risk exposure

- **Very High**
- **High**
- **Medium**
- **Low**
- **Very Low**

**Projection -** Considering risk management plans and environmental factors, the residual risk projection over the next fiscal quarter

- **Decrease**
- **Constant**
- **Increase**
Tracking of Appeals Correspondence in OBA is done on a weekly basis, including tracking of the number of days that a request from appeals (RFA) is outstanding. Generally RFAs are processed within the time frame required by policy (45 days). However it is not apparent that OBA has an escalation process in the event of difficulties with regards to appeals correspondence. Thus, even though the handling of individual appeals is a low risk item when we consider the monitoring approach currently in place, there is room for improvement in terms of summarizing appeals correspondence data and escalating where appropriate.

Executive Risk Owner(s): Andrea S.

Risk Management Team Participants: Bill C.

Sub Processes and Risk Statements

1. Sub-Process - Appeals Acknowledgement

A) If notification of an appeal filing is not received timely, OBA may process the benefit payment based on the original BD which could be incorrect given the outcome of the appeal. Taking action on the original BD could result in underpaying the participant/beneficiary or in overpaying the participant/beneficiary which, in turn, would result in recoupment, regardless of the appeals action.

2. Sub-Process - Implementation of decisions made by the Appeals Division

A) Decisions made by the Appeals Division may not be implemented accurately and/or timely.
   • Appeals decisions and actions may not be correctly implemented leading to potential hardship for the customer (e.g., recoupment of overpayment).
   • Appeals decisions and actions may not be implemented within established timeframes (30 days from notification), leading to risk of interest expense.
   • Benefit adjustments may not have been processed for all parties resulting in hardship to participants/beneficiaries and poor customer service.
   • Data used to calculate the benefit or decision of benefit is incorrect resulting in a revised calculation and BD. In some cases, new information may not have come out until after the BD is issued, resulting in a reissuance.
   • Delay in getting the appeals acknowledgement and/or appeals decision scanned in to IPS.


<table>
<thead>
<tr>
<th>Quarterly Rating:</th>
<th>Q2</th>
<th>Q3</th>
<th>Q4</th>
<th>Current</th>
<th>Projection</th>
<th>Baseline (Magnitude, Vulnerability)</th>
<th>Current (Magnitude and Vulnerability)</th>
<th>Risk Appetite: (Target Magnitude and Vulnerability)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(1.92 2.17)</td>
<td>(1.92 2.17)</td>
<td>(1.92 2.17)</td>
</tr>
</tbody>
</table>
Risk Acceptance

• You have just about completed your bottom’s up risk assessment and are preparing your risk response plans
• However due to cost benefit considerations and factors outside your agency’s immediate control you will need to accept some risk outside your target residual risk (risk appetite)
Target Residual Risk = Risk Appetite

- **Inherent risk** is the risk to an entity in the absence of any direct or focused actions by management to alter its severity.

- **Target residual risk** is the amount of risk that an entity prefers to assume in the pursuit of its strategy and business objectives, knowing that management will implement, or has implemented, direct or focused actions by management to alter risk severity.

- **Actual residual risk** is the risk remaining after management has taken action to alter its severity. Actual residual risk should be equal to or less than the target residual risk, as is illustrated in Figure 8.5.

Source: COSO ERM Framework Discussion Draft June 2016
Risk Acceptance

Figure 1: Risk Acceptance Graphic – No Risk Acceptance Needed

Risk Significance e.g., Magnitude X Likelihood

- Current Risk Tolerance
- Current Risk Appetite
- Current Residual Risk

Time

Figure 2: Risk Acceptance Graphic – Risk Acceptance Exists

Risk Significance e.g., Magnitude X Likelihood

- Current Residual Risk
- Current Risk Tolerance –
- Current Risk Appetite

Time

Risk Acceptance Exists
Portfolio View of Risk Acceptances

• Recommendation:
  – Portfolio views of risks that have been assessed are as useful as views of risks that have been accepted

  • Therefore, create an informative risk acceptance portfolio view for risks that are not controllable either due to external factors such as the economy, existing legislation, mandates outside your agency’s control.
Example - Residual Risk Heat Map Showing Risk Acceptances

Legend:
- Risk Acceptance
- No Risk Acceptance
Questions