



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.

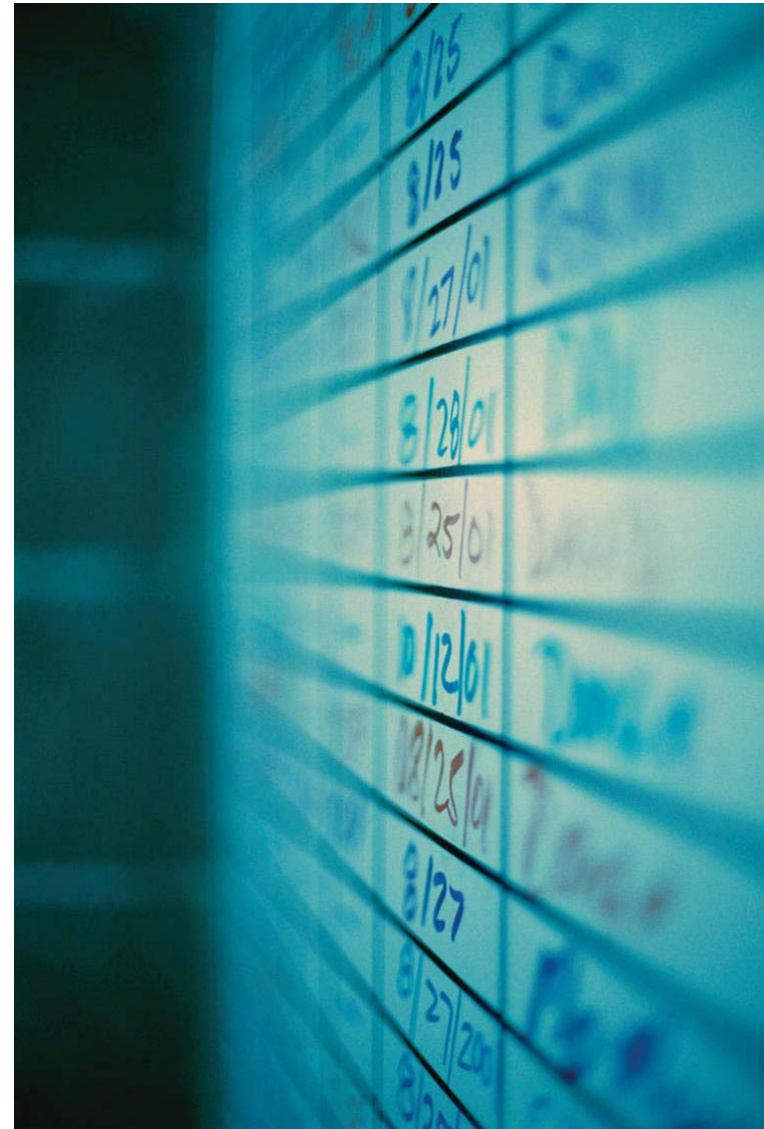
What is COSO?

- 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*



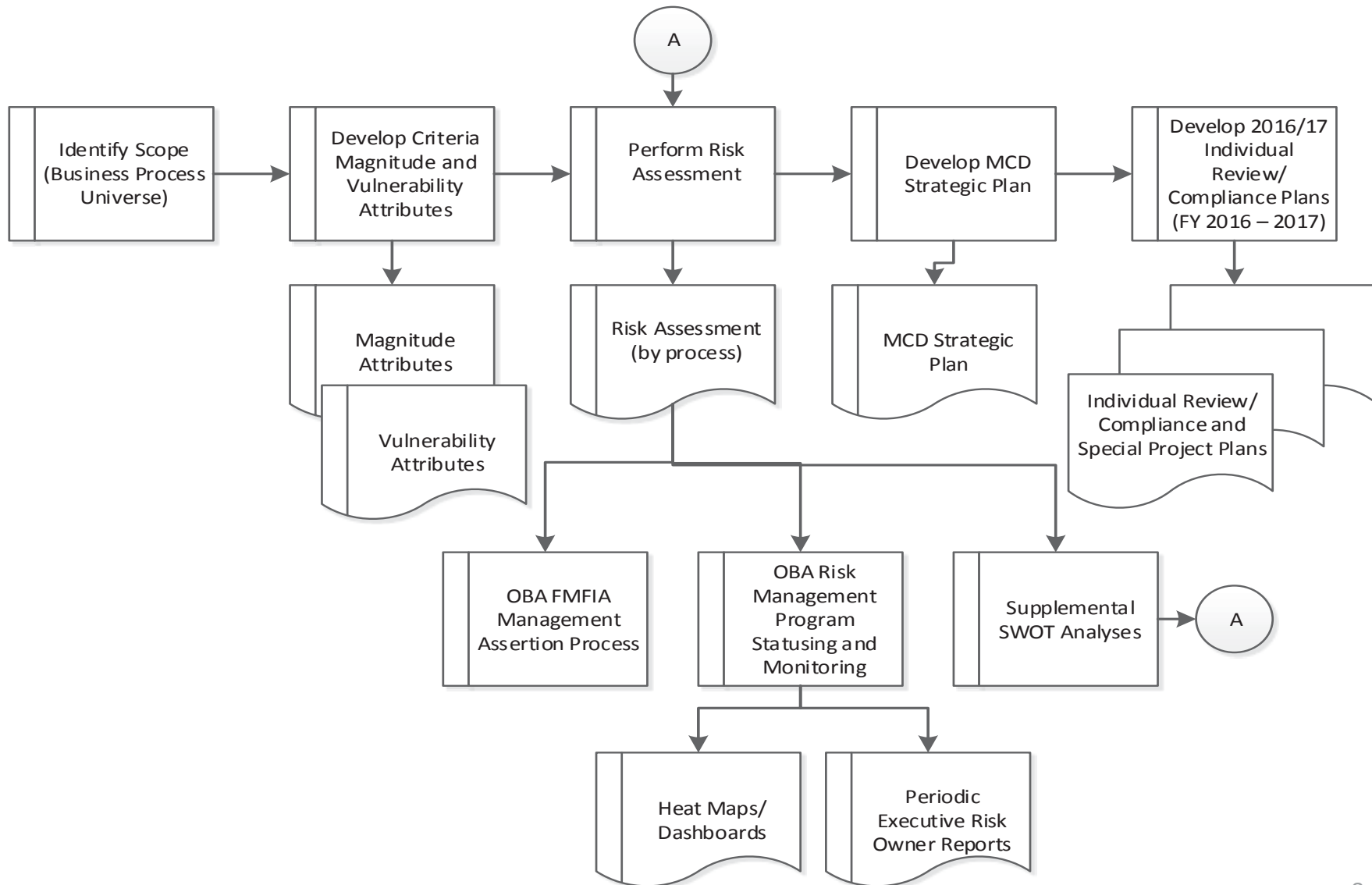
OIG Recommendations

- *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*

- *Source: Report on Internal Controls Related to the Pension Benefit Guaranty Corporation's Fiscal Year 2014 and 2013 Financial Statements Audit (AUD-2015-3 /FA-14-101-3), issued November 14, 2014*



OBA Approach to Risk Management



Develop Your Assessment Criteria

- Magnitude/Impact/Severity
- Likelihood/Vulnerability

Magnitude Criteria Matrix

Criteria	Financial Statement	Reputation	Legal/Regulatory	Customer	Employees	Other		Stakeholder
RATING						Strategic	Operational	Congress / DOL/Board of Directors
VERY HIGH (5)	>\$34.1M*	Sustained U.S. national (and international) negative media coverage (front page of paper or business section)	Major federal or state action/Fraud or bribery or other legal investigation/action	Major loss of customer satisfaction	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.	Major modification to strategy	Catastrophic impact on performance, such as major IT system failure/tampering/sabotage OR PBGC cannot pay benefits.	Major increase in hostile congressional hearings, major funding concerns, significant DOL or Board inquiries OR multiple reviews undertaken by internal and external audit inspection organizations OR significant attention from Board of Directors.
HIGH (4)	\$20M-\$34.1M	Negative U.S. national or international media coverage (not front page)	Federal or state investigations or action	Degradation of relationship with customers and severe customer satisfaction rating drop	Frequent/ significant workplace issues such as workplace safety and morale issues, stagnation and lack of growth opportunities	Modification to strategy	Severe impact on the business unit's operational performance OR large number of benefit payments cannot be made.	Degradation in confidence, congressional hearings, some funding concerns OR congressionally requested OR GAO or other audits occur. Significant attention from Director.
MEDIUM (3)	\$5M-\$20M	Negative media coverage in specific U.S. region or a foreign country, large plan involvement, many customers involved.	Few Federal or state investigations or action, routine costly litigation	Frequent, significant instances or sustained quality issues/conflict with customer(s)	Morale or satisfaction or commitment issues including salary OR benefits dissatisfaction.	Isolated modification to strategy as it relates to particular goals and customer service	Some damage requiring management attention. Minor system failure OR Benefit payments cannot be made to beneficiaries of certain plans.	Significant stakeholder reaction OR Congressional or OMB or DOL inquiries of PBGC.
LOW (2)	\$1M-\$5M	Localized negative impact on reputation (such as a small plan/several customers involved) but recoverable	Smaller regulatory, legal actions, or penalties/fines	Occasional negative issues/feedback from customer(s) not easily resolved	Career progression, salary issues, work-life balance issues	Isolated modification to strategy as it relates to BAPD and/or minor outcomes/services.	Noticeable, but limited impact on operations OR benefit payments cannot be made to individual beneficiaries.	Minor stakeholder reaction OR minor requests from stakeholder for information.
VERY LOW (1)	<\$1M	No press exposure	No regulatory or legal action	Infrequent issues/conflict with customer(s), easily resolved	Occasional employee issues, easily resolved	Course corrections easily achieved through normal business practices.	No loss of operational capability OR no impact on PBGC's ability to pay benefits.	Situation vulnerable to stakeholder reaction, but no measurable impact yet

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

Vulnerability Factors

	CONTROL EFFECTIVENESS & EFFICIENCY		PREVIOUS RISK EXPERIENCE	CAPABILITY				RATE OF CHANGE
RATING	Controls/ Mitigation	Monitoring/ Testing/Reporting	Costs, Audits, Regulatory	Training/Resources/Skills/ Knowledge	Third Party	Process Criticality	Systems/Data/Security/ Technology	Expansion or Contraction (business, people, process, systems)
VERY HIGH (5)	Controls are ineffective or do not exist	No controls monitoring, testing & reporting	>\$20M or other significant recent previous adverse experience, e.g. modified/adverse audit opinions, multiple material weaknesses.	NO in house staff to manage/mitigate the risk (no resources, skills or NO commitment to develop the capability) OR NO access to external resources to manage/mitigate	No knowledge/influence over third parties and/or third party relationships have high volatility.	Risk affects a critical process OR significant number of processes OR is a complex process OR process is immature, with extreme variability in execution/ outcome.	Significant system & data issues (performance, reliability, validity) OR security exposures OR technology is outdated, inefficient and ineffective	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
HIGH (4)	Controls are minimally effective. For example, detect but do not prevent exposure	Minimal controls monitoring, testing & reporting	\$5M or other major recent previous adverse experience, e.g. one or more material weakness but no adverse opinion	LIMITED in house staff to manage/mitigate the risk (limited resources, skills and a LIMITED commitment to develop the capability) OR LIMITED access to external resources to manage/mitigate	Limited Knowledge/ influence over third parties and/or third party relationships are volatile.	Risk affects a critical process OR major number of processes OR is a complex process; Process is somewhat immature, is not systematic, with significant variability in execution/outcomes.	Major system & data issues (performance, reliability, validity) OR security exposures OR Technology is Minimally efficient and effective	Risk is managed by or directly impacts people, processes, systems or divisions that have experienced a major rate of change over the last 6 months
MEDIUM (3)	Controls are somewhat effective. Can detect some risk.	Some controls monitoring, testing & reporting, but inconsistent	\$500K or other moderate recent or previous adverse experience, e.g. significant deficiencies/audit findings	MODERATE in house staff to manage/mitigate the risk (moderate resources, skills or MODERATE commitment to develop the capability) OR MODERATE access to external resources to manage/mitigate	Minor knowledge/ influence over third parties and/or relationships are somewhat volatile.	Risk affects a non critical process OR moderate number of processes OR is a simple process. Process is somewhat mature, somewhat systematic, with some variability in execution and outcomes.	Moderate system & data issues (performance, reliability, validity) OR security exposures OR Technology is somewhat efficient and effective	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
LOW (2)	Controls detect & prevent risk	Sufficient monitoring, testing & reporting	Minor recent previous adverse experience, e.g. a reportable condition or finding	SUFFICIENT in house staff to manage/mitigate the risk (sufficient resources, skills or commitment to have the capability) OR SUFFICIENT access to external resources to manage/mitigate	Sufficient knowledge/ influence over third parties and/or relationships have occasional issues.	Risk affects a non critical process OR minor number of processes OR is a simple process. Process is significantly mature, predominately systematic with limited variability in execution and outcomes.	Few system & data issues (performance, reliability, validity) OR security exposures OR Technology is somewhat efficient and effective	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
VERY LOW (1)	Controls are very effective at detecting & preventing risk	Extensive monitoring, testing & reporting	No recent previous adverse experience	More than SUFFICIENT in house staff to manage/mitigate the risk (sufficient resources, skills and commitment to the capability) OR more than SUFFICIENT access to external resources to manage/mitigate	Very sufficient knowledge/influence over third parties and/or no third party relationship issues.	Risk affects a non critical process OR minor number of processes OR is a simple process. Process is quite mature, systematic, little/no variability in execution or outcomes, repeatable, sustainable.	No system & data issues (performance, reliability, validity) OR Security exposures OR Technology is efficient and effective	Risk is managed by or directly impacts people, processes, systems or businesses that have experienced no rate of change over the last 6 months

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)	Identify Risk Interrelationships and Interdependencies
<p>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.</p> <p>There may be an unwavering determination to spend funds the way they were initially planned</p> <p>An emphasis may be placed on funding/accomplishing daily tasks without considering the impact on the strategic goals</p> <p>The results of expenditure monitoring, such as status of funds reporting, may not be analyzed to determine expenditure's effectiveness</p> <p>Funds which are limited may be improperly allocated to lower priority projects</p> <p>Monitoring and reviewing fund usage may not occur to ensure that funds are expended as planned</p> <p>Monitoring (testing) by BAPD of processes, controls and risk related to budget execution may be minimal</p> <p>The availability of funds may be subject to continuing resolutions issues</p>	<p>The CFS System</p> <p>Comprizon Suite -- acquisition management application</p> <p>References:</p> <ul style="list-style-type: none"> • 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 Obligor Procedures for PBGC Procurements <div style="border: 1px solid black; padding: 5px; margin-top: 20px; display: flex; justify-content: space-between;"> Prepared by: Cate H. Date: 2/19/2016 </div> <div style="border: 1px solid black; padding: 5px; margin-top: 5px; display: flex; justify-content: space-between;"> Reviewed by: Bernice Lemaire Date: 02/21/2016 </div>

Risk Profile - Mega Process Name

Budget - Execution

Assess Gross Risk Magnitude [Rate Scale: VH=5, H=4, M=3, L=2, VL=1]								
Financial <i>Est Impact to Financial Statements</i>	Reputation	Legal/ Regulatory	Customer	Employees	Strategic	Operational	Stake- holder Confidence	Overall Magnitude Rating: 1.13 Very low
2	1	1	1	1	1	1	1	
Assess Vulnerability [Rating Scale: VH=5, H=4, M=3, L=2, VL=1]								
Vulnerability Factors		Rating	Vulnerability Factors		Rating	Overall Vulnerability Rating: 1.25 Very low Recommended Alternative / Improved Risk Mitigation Techniques: (TBD)		
Controls / Risk Mitigation Measures: • Multiple people review requisitions before they are finalized		1	Third Party Reliance: • N/A no third party relationship		1			
Controls Monitoring, Testing and Reporting: • Very low risk because the movement of money for requisitions is very slow, so there is plenty of time to review and make corrections		1	Process Criticality: (e.g., Is process mission critical?)		2			
Previous Risk Experience:		1	System, Data, Security, Technology: • The system that tracks Budget Execution is not BAPD-led • Occasional/rare issues of data being incorrect or the database being down		1			
Training, Resources, Skills and Knowledge: • Staff in charge of Budget Execution is very knowledgeable in the subject • Would benefit from additional staff knowing the process		2	Rate of Change:		1			
Other:								

Develop Useful Dashboards and Status Reporting Methods

Excel Dashboard with Conditional Formatting

FY 2015 OBA UNIVERSAL RISK ASSESSMENT																								
Title: Magnitude and Vulnerability Risk Assessment for BAPD Processes																								
Process #	Process Name	Sub Process Name	Significance (Mx)	Magnitude										Vulnerability								Strategic Goal One (Preserve Plans and Pensioners)	Strategic Goal Two (Pay Pension Benefits On Time and Accu)	Strategic Goal Three (Maintain High Standards of Stewardship and Accountability)
				Financial Statement Impact	Reputation	Legal/Regulatory	Customer	Employees	Strategic	Operational	Stakeholder Confidence	Magnitude Overall	Controls/ Risk Mitigation Measures	Controls, Monitoring, Testing Reporting	Prior Risk Experience	Training, Resources, Skills Knowledge	Third Party Reliance	Process Criticality	System, Data, Security & Technology	Rate of Change	Vulnerability Overall			
2	Appeals Correspondence	Appeals Acknowledgement	5.12	3	3.33	2.67	2.67	2.33	2.33	1.33	2	2.46	2.33	4.33	1.33	1.67	1.33	1.33	2.33	2	2.08			
2	Appeals Correspondence	Implementation of decisions made by the Appeals Division	3.09	1.33	2	1	2	1	1.67	1	1	1.38	3	3.67	1	2	1	3	1.67	2.67	2.25			
3	Benefit Adjustments	Analyze Plan Documents	1.75	1	1	1	1	1	1	1	1	1	2	2	1	2	2	2	2	1	1.75			
3	Benefit Adjustments	Obtain Data	2.66	1	1.8	1	2	1.6	1.4	1.2	1.8	1.5	1.8	1.8	1.4	1.8	2.2	2.2	1.6	1.2	1.78			
3	Benefit Adjustments	Analyze Data and Funding for PC 3	2.10	1	2.4	1.4	1.6	1	1.2	1	2.4	1.38	2	1.8	1.4	1.8	2	1.6	1	1	1.53			
3	Benefit Adjustments	Identify Current Payees for Benefit Adjustments	1.96	1	1.6	1.2	1.6	1	1.2	1.2	1.6	1.38	1.4	1.2	1.4	1.8	2	1.4	1.2	1	1.43			
3	Benefit Adjustments	Prepare Estimated Benefits Calculation Tool	2.00	1	1.6	1.2	1.6	1	1	1	1.6	1.25	1.4	1.8	1.6	1.6	1.8	1.8	1.4	1.4	1.6			
4	Benefit Determination Letters	Create Early BDL Database and Issue Early BDLs	3.00	1	2	1	2	1	1	1	3	1.50	2	2	2	2	2	2	3	1	2.00			
4	Benefit Determination Letters	Review Actuarial Case Report and Issue BDLs	6.00	2	3	2	3	1	1	1	3	2.00	4	4	3	4	1	3	4	1	3.00			
4	Benefit Determination Letters	Determine Net Overpayment/Underpayment for Annuities	10.42	3	4	3	4	2	2	2	3	2.88	4	4	5	3	4	3	4	2	3.63			
4	Benefit Determination Letters	Determine Net Overpayment/Underpayment for Lump Sums	7.56	4	4	2	4	1	2	2	3	2.75	3	4	5	1	2	3	2	2	2.75			
4	Benefit Determination Letters	Issue Revised Benefit Determination Letter	1.69	1	1	1	1	1	1	1	2	1.13	2	1	1	1	1	4	1	1	1.50			
4	Benefit Determination Letters	Issue Limited Scope BDL	1.00	1	1	1	1	1	1	1	1	1.00	1	1	1	1	1	1	1	1	1.00			
4	Benefit Determination Letters	Mid-Valuation Benefit Determination Letters	4.22	1	1	1	1	1	1	1	3	1.25	5	5	4	4	1	4	3	1	3.38			
4	Benefit Determination Letters	Maintain BDL Review File for Large Plans	1.00	1	1	1	1	1	1	1	1	1.00	1	1	1	1	1	1	1	1	1.00			
5	Benefit Payments	Determine Eligibility and Issue Application	2.66	1	2	1	2	1	1	1	1	1.25	1	1	2	2	2	2	3	1	2.13			

OBA Quarterly Risk Management

Status Report

Executive Risk Owner

Andrea S.

October 4, 2016

Appeals Correspondence

**Do not disclose outside of OBA, without Chief of OBA
permission**

Format version 3.0
Format Last updated
10/19/2016



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

Cathy Kronopolus, CBA

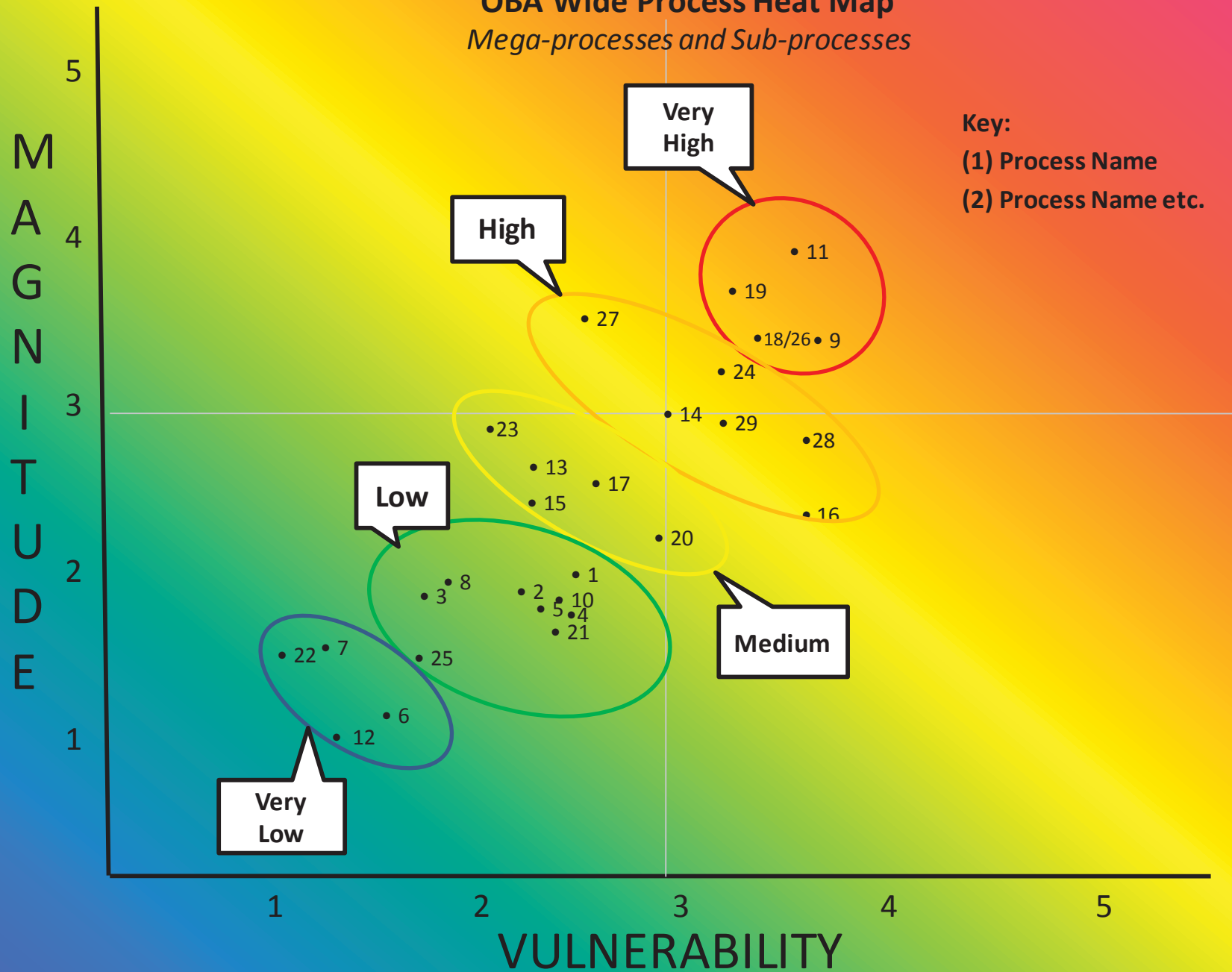
Date: _____

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

#	Process Risk Name	Quarterly Rankings					Executive Risk Owner	Upcoming Risk Management Milestone	Risk Management Summary Schedule
		Q2	Q3	Q4	Current	Proj.			
2	Appeals Correspondence						Andrea S.	Quarterly escalation report of appeals correspondence	◆ Quarter end, beginning first quarter in FY 2017

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

Top OBA Risk Report: Appeals Correspondence								
Quarterly Rating:	Q2	Q3	Q4	Current	Projection	Baseline (Magnitude, Vulnerability)	Current (Magnitude and Vulnerability)	Risk Appetite: (Target Magnitude and Vulnerability)
						(1.92 2.17)	(1.92 2.17)	(1.92 2.17)

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.

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

Figure 8.5: Inherent, Target, and Residual Risk



Source: COSO ERM Framework Discussion Draft June 2016

- *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.

Risk Acceptance

Figure 1: Risk Acceptance Graphic – No Risk Acceptance Needed

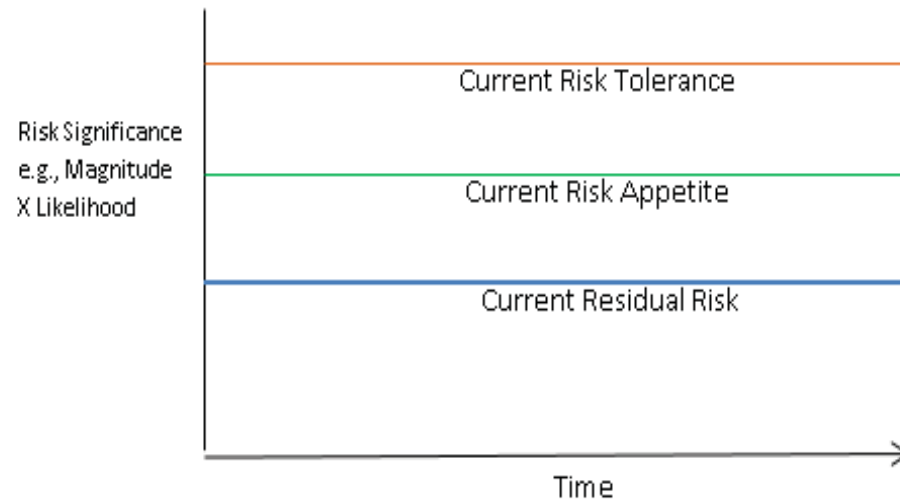
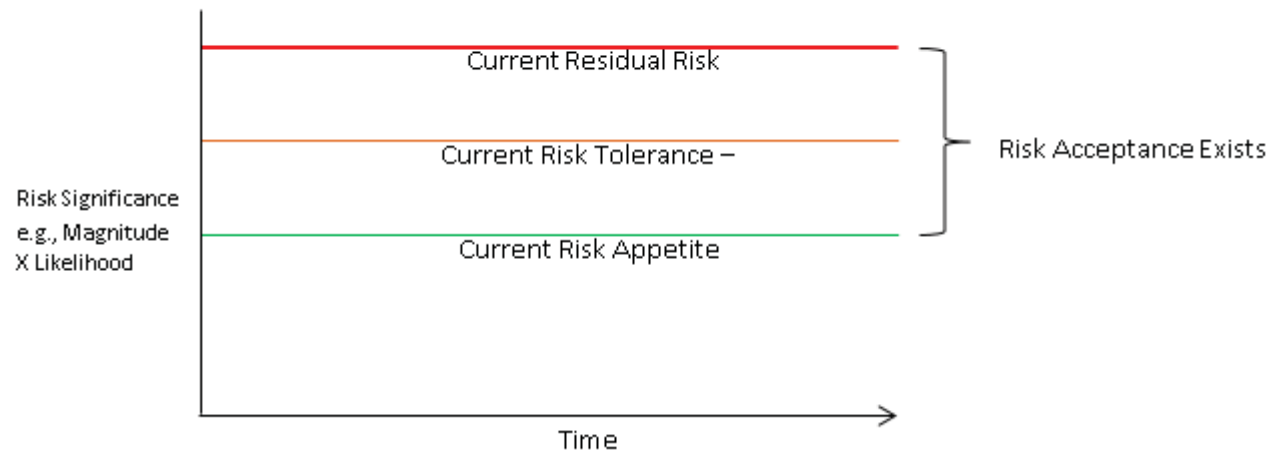


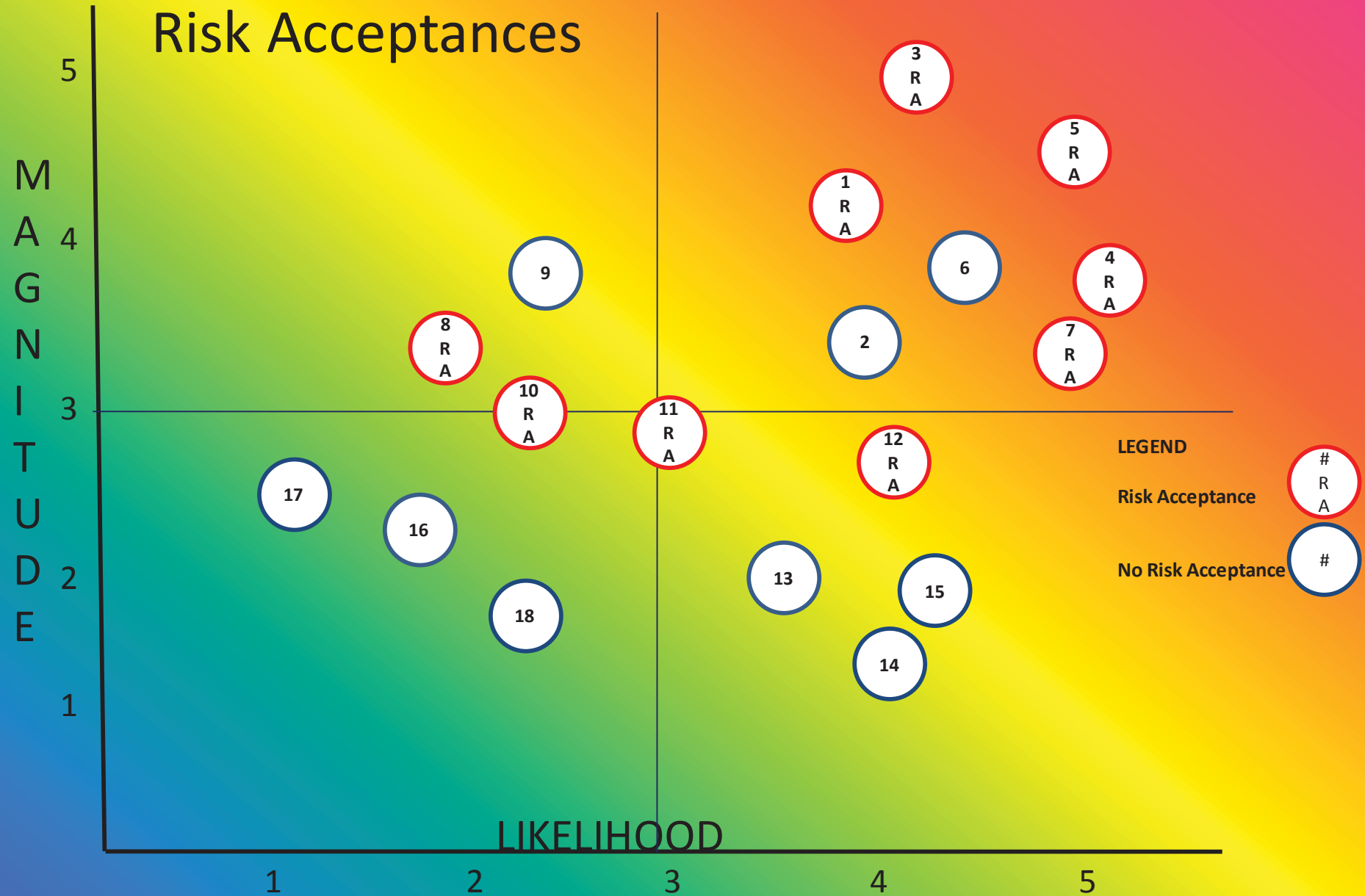
Figure 2: Risk Acceptance Graphic – Risk Acceptance Exists



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



Questions