May 16, 2016

MEMORANDUM TO ALL STAFF

FROM: Robert A. Westbrooks
Inspector General

Digitally signed by Robert A. Westbrooks

SUBJECT: OIG Enterprise Risk Management Program

Background

This memorandum is to document the establishment and implementation of an Enterprise Risk Management program at the PBGC Office of Inspector General. By adopting a portfolio view of risks, ERM will enable our office to:

- lead by example,
- provide for more effective risk management and internal control in accordance with *OMB Circular A-123*,
- align management activities with the CIGIE *Quality Standards for Federal Offices of Inspector General* (also known as the "*Silver Book*"),
- concentrate efforts towards key points of failure and reduce or eliminate the potential for disruptive events,
- allow for risk-based planning, and
- protect the PBGC OIG brand ("independent, positive engagement") and identify opportunities to create value.

The framework for this program is based on (the soon-to-be issued) *OMB Circular A-123*, *The Orange Book, Management of Risk – Principles and Concepts* (October 2004, HM Treasury), and *the Committee of Sponsoring Organizations of the Treadway Commission's* (COSO) *Enterprise Risk Management Framework.* This memorandum describes responsibilities and governance structure, the foundation of this program, the components of this program, the external and internal environment to provide necessary context for assessment of OIG risks, the methodology for developing our risk appetite, and the methodology for developing our risk profile.

Our office is at what would be considered the initial stage of the RIMS ERM maturity model. We aspire to evolve to the repeatable and managed stages and beyond. Our entry at the initial

stage requires us to recognize the limitations of this effort. This initial effort is unabashedly imperfect and imprecise. Our best course of action at this point, though, is to begin with ERM even if some elements of this program are not yet defined. Experience will be our guide and this program will mature over time through sustained commitment and trial and error.

Responsibilities and Governance Structure

One of the responsibilities of an Inspector General under the IG Act is to provide leadership to promote economy, efficiency, and effectiveness. Under this ERM program, it is the duty and responsibility of the Inspector General to encourage a risk-aware culture that stresses individual accountability at all levels. It is the duty and responsibility of the Assistant Inspectors General to manage risk in their program areas. This includes identifying, analyzing, and evaluating risks and presenting risk response options to the Inspector General. Each OIG employee is encouraged to be open, candid, and fact-based in discussing risk issues, making all relevant facts and information available so that the Inspector General can consider all options and make informed decisions. We are all accountable for speaking up and escalating concerns to management about risks. If, for any reason, an OIG employee prefers confidentiality or anonymity, the employee may report the risk concerns to the OIG Employee Advisory Committee, who will ensure this information is reported to the Inspector General.

Given our size, this program will be managed directly by the Inspector General in consultation with the Chief of Staff. The Inspector General may delegate, in writing, some activities required under this program, such as maintenance of the risk profile or monitoring performance, but will not delegate ultimate responsibility for OIG enterprise risk management.

Foundation of the OIG Enterprise Risk Management Framework

Figure 1: OIG Value Framework

Our value framework and code of conduct are the core of our organizational philosophy and set the tone and values of our office. The value framework encompasses our commitment to a culture that is "people focused, process oriented, and performance driven" and to a vision of "providing deep knowledge and sensible solutions through independent, positive engagement."

Our code of conduct documents the expectation that each OIG employee firmly adheres to our values of respecting all individuals, committing to personal excellence, and acting with honesty and honor even when nobody is looking. Included in this concept is the requirement that an employee's job performance must at all times manifest the highest standard of these values.

The CIGIE *Quality Standards for Federal Offices of Inspector General* sets forth the overall quality framework for managing, operating, and conducting the work of an OIG. These standards include a requirement that "the IG should provide for an assessment of the risks the OIG faces from both external and internal sources."

GAO's latest *Standards of Internal Control* (also known as the *Green Book*) became effective for federal agencies beginning FY 2016. The updated *Green Book* adopts the *COSO 2013 Internal Control–Integrated Framework*. In addition, OMB is finalizing its guidance, *Circular A-123*, which includes detailed guidelines for the evaluation of systems of internal control, will emphasize the need to manage risk and internal control in both financial and nonfinancial areas, and will require federal agencies to implement enterprise risk management practices.

Components of the OIG ERM Framework

Our ERM framework consists of seven components. They are:

Establish the Context - understanding and articulating the internal and external environments of the organization. The environment may generate risks that cannot be controlled, or constrain the way the OIG responds to a risk.

Initial Risk Identification - using a structured and systematic approach to recognizing where the potential for undesired outcomes or opportunities can arise.

Analyze and Evaluate Risks - considering the causes, sources, probability the risk will occur, the potential positive or negative outcomes, and then prioritizing the results of the analysis.

Develop Alternatives, if applicable - systematically identifying and assessing a range of risk response options guided by risk appetite.

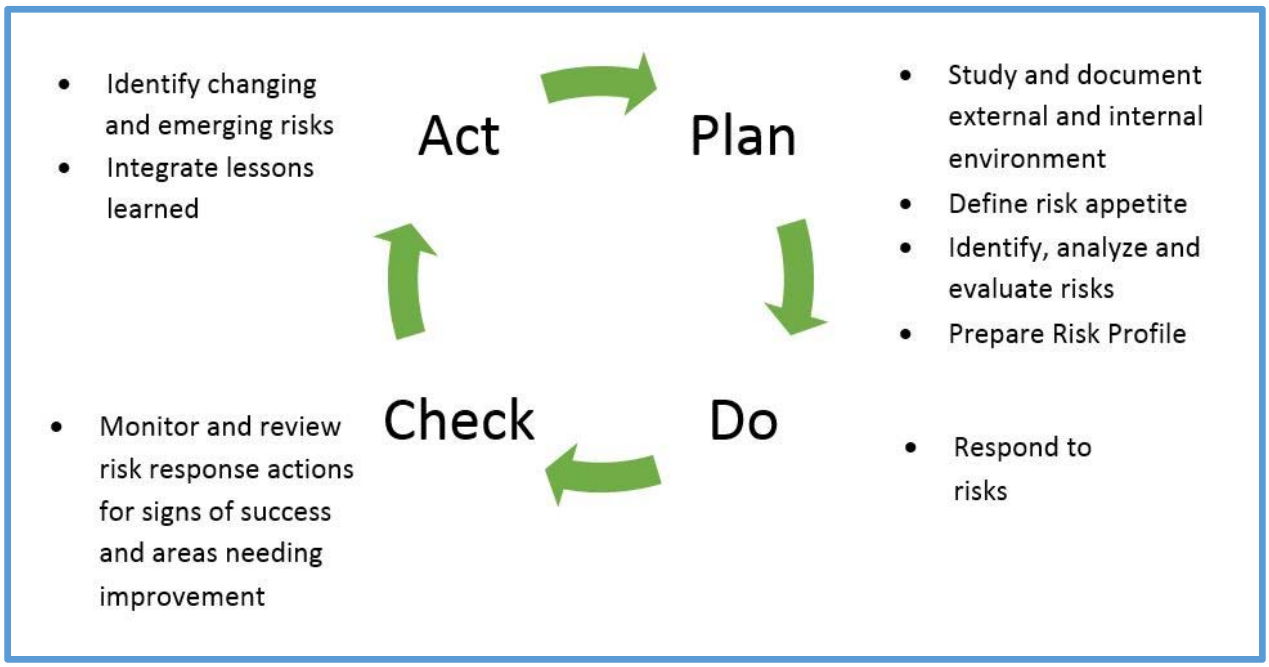
Respond to Risks - making decisions about the best options(s) among a number of alternatives, and then preparing and executing the selected response strategy. Risk responses will involve one or more of the following: acceptance, avoidance, reduction, sharing.

Monitor and Review - evaluating and monitoring performance to determine whether the implemented risk management options achieved the stated goals and objectives.

Continuous Risk Identification – identifying risk throughout the year. Risk identification is an iterative process and a shared responsibility of each employee.

These components can be organized into the Deming PDCA continuous quality improvement model as follows:

Figure 2: Summary of ERM Components into Deming PDCA Model



Establishing the Context: External and Internal Environment

PBGC was established under the Employee Retirement Income Security Act of 1974 as a self-financing, wholly-owned Federal Government corporation within the Department of Labor to administer the pension insurance program. ERISA requires that PBGC (1) encourage the continuation and maintenance of voluntary private pension plans, (2) provide for the timely and

uninterrupted payment of pension benefits to participants and beneficiaries, and (3) maintain premiums at the lowest level consistent with carrying out PBGC's obligations.

PBGC is headed by a Director who is appointed by the President and confirmed by the Senate. The Corporation is governed by a Board of Directors which is composed of the Secretary of Labor, the Secretary of the Treasury, and the Secretary of Commerce. The Secretary of Labor serves as the Chairman of the Board. Each Board Member designates an official, not below the level of Assistant Secretary, to serve as the Board Member's Representative who may act on behalf of the Board Member. The Director submits the Corporation's budget to the Chair of the Board for review and approval.

PBGC is currently responsible for protecting the pensions of more than 40 million American workers in nearly 24,000 private sector defined benefit plans. The Corporation receives no general tax revenues. It manages about $88 billion in assets financed by insurance premiums from its single-employer and multiemployer pension insurance programs, investment income, and the assets of terminated single-employer plans. In 2015, the Corporation paid $5.6 billion in monthly retirement benefits to nearly 826,000 retirees in some 4,700 single-employer plans and it paid $103 million in financial assistance to 57 multiemployer plans.

PBGC faces significant, long-standing, and well-known risks. Both pension insurance programs face serious long-term funding challenges with the premium base declining as fewer employers offer defined benefit plans. In 2003, the Government Accountability Office designated the single-employer pension insurance program as high risk, and GAO added the multiemployer pension insurance program to its high risk list in 2009. At the end of FY 2015, PBGC's net deficit in the combined programs was $76 billion with exposure of $238 billion for projected future underfunded plans. According to PBGC projections, it is more likely than not that the multiemployer pension insurance program will run out of money by 2025. PBGC insolvency projections are highly dependent on the stochastic projection of many, highly variable factors, such as future interest rates, future equity returns, and future decisions by plan sponsors.

The PBGC Office of Inspector General was created under the 1988 amendments to the Inspector General Act of 1978. We provide independent and objective audits and investigations to help the Congress, the Board of Directors, and PBGC protect the pension benefits of American workers.

We are organizationally independent from the Corporation, with the Inspector General reporting to the Board of Directors through the Chairman. Under Public Law 112-141, the Inspector General must attend at least two Board meetings a year "to provide a report on the

activities and findings of the Inspector General, including with respect to monitoring and review of the operations of the corporation."

Our audit staff is led by an Assistant Inspector General for Audit, our investigative staff is led by an Assistant Inspector General for Investigations, and the OIG is supported by an Administrative Officer. The OIG executive leadership team consists of the Inspector General, Chief of Staff, and Chief Counsel**.** We have 25 FTE positions, which are currently allocated as follows: 13 in the Office of Audit, 4 in the Office of Investigations, and 8 in the Front Office. Our FY 2016 budget is $6.3 million. The OIG submits its budget to the Corporation for inclusion (but not review) in the Corporation's budget submission to the Department of Labor.

As a federal OIG, much of our annual audit plan and resources are dedicated to statutorily required projects including the financial statement audit, the Federal Information Security Modernization Act evaluation, and the Improper Payments Information Act audit. Statutory audit requirements evolve over time. In FY 2015, for example, we were tasked along with other federal OIGs with completing an evaluation of the implementation of the requirements of the Cybersecurity Act of FY 2015. In the past, we have also received congressional requests to review the actions of PBGC in processing terminated plans. Due to the subject matter of these reviews, there is typically high public interest and time is of the essence.

The IG Act and Government Auditing Standards require each audit organization to obtain an external review of its system of quality control every three years and make the results publicly available. In an external peer review of the PBGC OIG's audit program for the year ending September 30, 2012, we received the peer review rating of "pass with deficiencies." The "pass with deficiencies" rating means that the external reviewer determined that our system of quality control was suitably designed, and our adherence to this system provided reasonable assurance that we performed work and reported results in accordance with professional standards in all material respects with the exception of a certain deficiency or deficiencies that are described in the report. The National Science Foundation OIG is conducting our peer review for the period ending September 30, 2015.

Our office has experienced significant turnover in staff and leadership in the past two years. Staff turnover in 2014 was 9 employees (or 30 percent). In May 2015, a new Inspector General was appointed. At the time, there were 8 staff vacancies. Leadership turnover since May 2015 has been 100 percent with five managers leaving the PBGC OIG, the Deputy Inspector General/Counsel being reassigned to Chief Counsel to the IG, and an audit manager being reassigned to quality assurance manager. We hired 11 new employees, including two newly created positions: chief of staff and senior investigative counsel.

The OIG ecosystem includes independent procurement, human resources, and IT functions. Chief Counsel to the IG serves as the OIG contracting officer, and our human resources function is outsourced to the Interior Business Center. We operate our IT systems as a subdomain on the PBGC enterprise domain, with a one-way trust relation from OIG to PBGC, and separated and secured through a firewall. OIG maintains its own email/Exchange server, file servers, and instances of Case Management Tracking System, TeamMate, domain controllers, and other utilities.

Risk Appetite

Defining risk appetite is challenging in an OIG environment, particularly when applying the COSO definition of risk appetite ("the amount of risk, on a broad level, an organization is willing to accept in pursuit of value"). The Inspector General, in consultation with the Assistant Inspectors General, will set the OIG risk appetite as part of the annual (calendar year) performance planning process. The risk appetite is essential to planning the best use of our available resources. It will be used to establish threshold criteria for investigations and audits, to examine performance measures (and adjust, if necessary), and to allocate resources for competing administrative projects and monitoring activities.

Given the reliance that is placed upon our audits and investigations by the Congress, the Board, management, the public, and prosecutors, we will operate within a low overall risk range. We will reduce to the maximum possible level our reputational risks, particularly concerning compliance with Government Auditing Standards and CIGIE Quality Standards.

One of the considerations affecting risk appetite is risk tolerance. According to COSO, this is defined as the "acceptable level of variation an entity is willing to accept regarding pursuit of its objectives." Our acceptable level of variation regarding OIG economy and efficiency is greater than our acceptable level of variation regarding compliance with professional standards and meeting the information needs of our stakeholders. As an organization, we will be ruthlessly committed to quality.

Risk Profile

ERM is a process, not an event. One major tool to document the process is a risk profile. At a larger organization with significantly more risks, a risk register may be maintained as a complete inventory of all risks. Given our size and the maturity level of our ERM program, we will develop a risk profile which identifies, assesses, and prioritizes our major risks from a portfolio perspective.

We will not prescribe a format for the OIG initial risk profile, but will examine and experiment with the formats used in other organizations to determine what format best fits our needs. At a minimum, the risk profile will identify objectives, identify the risk, assess inherent risk, identify risk response, assess residual risk, and identify the proposed action.

For the OIG initial risk profile, we will use the following assessment categories:

Impact

High (3): the impact could preclude or highly impair the OIG's ability to achieve one or more of its statutory responsibilities, objectives or performance goals;

Medium (2): the impact could significantly affect the OIG's ability to achieve one or more of its statutory responsibilities, objectives or performance goals; and

Low (1): the impact will not significantly affect the OIG's ability to achieve one or more of its statutory responsibilities, objectives or performance goals.

Likelihood

High (3): the risk is very likely or reasonably expected to occur;

Medium (2): the risk is more likely to occur than unlikely; and

Low (1): the risk is unlikely to occur**.**

The risk profile will multiply the impact factor times the likelihood factor and the product will be the risk profile score. For example, a risk which is scored as high impact, low likelihood would be scored as 3 x 1, or 3.

According to OMB Circular A-123, our risk profile should include the following objectives:

Strategic Objectives: relating to the strategic goals and objectives aligned with and supporting the Agency's mission.

Operations Objectives: relating to the effective and efficient use of the Agency's resources related to administrative and major program operations.

Reporting Objectives: relating to the reliability of the Agency's reporting.

Compliance Objectives: relating to the Agency's compliance with applicable laws and regulations.

For our purposes, we define our relevant risk categories as:

1. Reputational (which encompasses strategic, operations, and reporting objectives) ,
2. Program Performance (which encompasses operations, reporting, and compliance objectives),
3. Human Capital (which encompasses strategic, operations and compliance objectives),
4. Technology (which encompasses operations, reporting, and compliance objectives).

Using these risk categories, we will complete our risk profile by August 31, 2016.

Conclusion

This program will significantly improve OIG leadership's ability to manage risks and allocate our limited resources. The establishment of this program is just the first step in a long journey.

Thank you in advance for your full participation.