Internal Audit Plan CY2017

Internal Audit Division
Office of Enterprise Risk Management
Federal Retirement Thrift Investment Board
November 29, 2016

Agenda

- Lines of Defense
- Audit Lifecycle
- Requirements
- Methodology
- Results
- Proposed Audits

Risk Management “Lines of Defense”

1st Line of Defense

Management

- Primary accountability for identifying, measuring, managing and mitigating risks
- Promote strong risk and control culture
- Implement governance and oversight, within specific businesses and across the enterprise

2nd Line of Defense

Risk and Control Functions

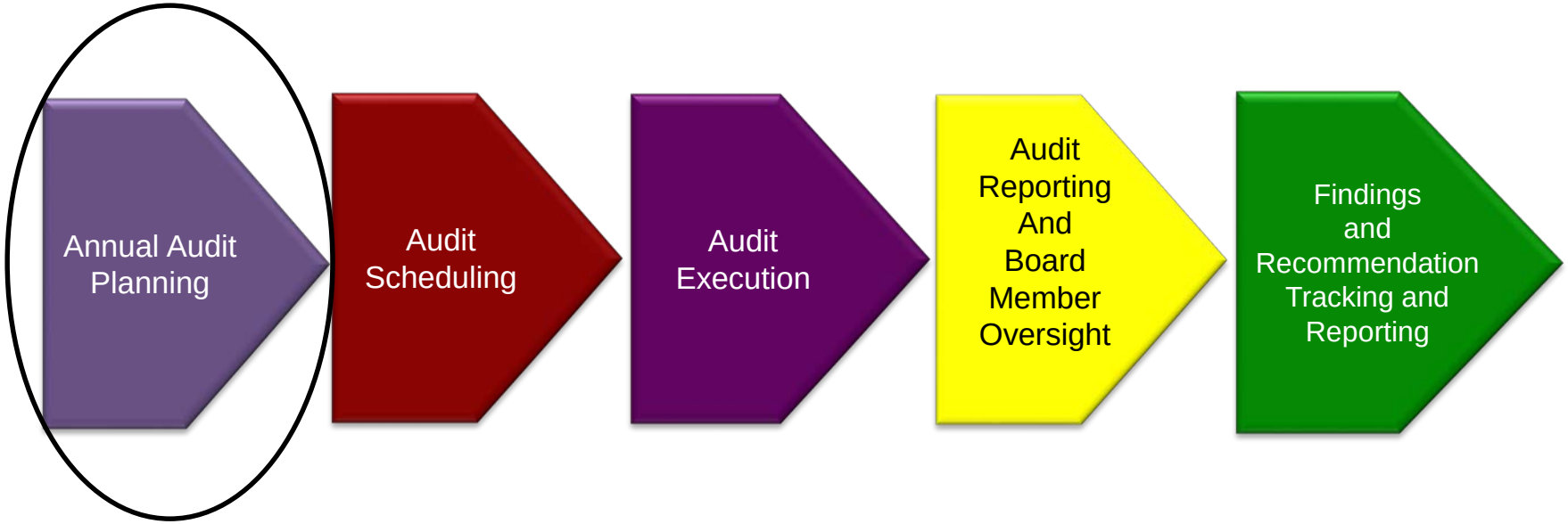
- Act as independent set of eyes and trusted advisor to help management operate more effectively as a 1st line of defense
- Advise/Consult/Oversee/Monitor
- Close and continuous relationships
- Mapping of key business operations
- Evaluation of design of controls
- Identifying and tracking gaps
- Policy and procedure development, modification and implementation
- Drive technology risk and associated reporting
- Privacy and info. security programs

3rd Line of Defense

Internal Audits

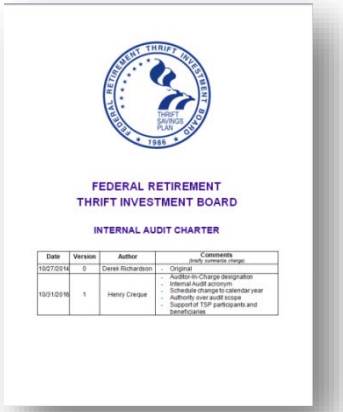
- Independently, objectively and systematically review and test the effectiveness of the control environment
- Identify, escalate and report risk and control deficiencies
- Perform risk-based assurance testing on remediation action plans
- Keep the ELC and the Board Members fully informed about and deficiencies noted in FRTIB’s programs and operations and opportunities for improvement
- Formal engagement with The Board Members
- Monitoring and tracking corrective actions to address findings and recommendations

Internal Audit Lifecycle



Requirements

- Pursuant to Federal Retirement Thrift Investment Board (FRTIB) Internal Audit Charter, Internal Audit (IA) Division is required to conduct a risk analysis and propose CY2017 Audits for Board Members Approval.
- The Institute of Internal Auditors interpretation of Standard 2010, “Planning,” states as part of establishing a risk-based internal audit plan, “*If a framework does not exist, the chief audit executive uses his/her own judgement of risk after consideration of input from senior management and the board.”*


FEDERAL RETIREMENT
THRIFT INVESTMENT BOARD

INTERNAL AUDIT CHARTER

Date	Version	Author	Comments (briefly summarize change)
10/07/2014	0	Derek Richardson	- Original
10/31/2016	1	Henry Creque	- Auditor-in-Charge designation - Internal Audit acronym - Schedule change to calendar year - Authority over audit scope - Support of TSP participants and beneficiaries

Internal Audit Risk Assessment Methodology

Assessment of Auditable Areas:

- Identify FRTIB business processes (IA conducted an analysis of all developed policies and procedures)
- Review the FRTIB Key Business Processes 'Who's On First' to identify business processes not covered in policies and procedures
- Participate in process discussions with each Office Directors

Risk Assessment:

- Participate in risk discussions with Office Directors and FRTIB management to identify audit considerations
- Review of industry data on potential risks that may affect FRTIB
- Apply professional judgement after considering input received from FRTIB Staff, DoL, KPMG.
- Applied a scoring methodology to the 182 business processes

Development of Plan:

- Assign risk rating by Office using established criteria:
  - Prior audits
  - Open audit findings
  - Notification
  - Etc.
- Review DoL Audit Plan to eliminate duplication of effort
- Create Plan based on available resources

Results

- IA ranked the 182 processes by Office.

Office	Number of Processes	IA Highest Risk Process by Office
OTS	54	Access Controls Procedures
OCFO	21	Procurement Planning Process
OGC	7	PII Data Breach Response
OEP	5	Acquisition Policy
ORM	41	Agency Travel Card
OCE	6	Social Media Procedures
OERM	7	External Audit and Oversight Coordination
OPOP	25	Lost Participants
OI	11	Audit and Due Diligence Review Procedure
OEA	2	Congressional Correspondence Procedure
OED	3	Board Meeting Preparation

Proposed Audits for CY2017

- IA reviewed U.S. Department of Labor Employee Benefits Security Administration (EBSA) FY2017 TSP Fiduciary Oversight Program and removed overlap
- IA propose the following audits in CY2017

Office	Audit	Primary Objective
ORM	Agency Travel Card	Assess the internal controls for the travel, and centrally billed accounts to reduce the risk of improper or erroneous purchases and payments.
OTS	Release Management Process	Assess the controls governing the process of software builds through the environment from development to production; including the testing and deployment of software releases.
OTS*	Omni Application	Evaluate the application controls for the Omni Record Keeping System as it relates to, Application Security, Business Processes Controls, Interface Controls, and Data Management System Controls.
OCFO*	Procurement and Contract Management	Evaluate the process for the procurement of goods and services by the FRTIB.
OCFO*	Vendor Management	Evaluate how third-party contractors are evaluated, supervised, and managed throughout the life of the contract and to evaluate the due diligence, oversight, and assess potential risk of third-party contractors performed by FRTIB offices.
OGC*	Cyber Security Incident/Breach Response	Assess the Agency's Incident Response program and its ability to deploy resources to respond to such a threat.

*Prior approved Audits

Questions