Executive Committee

Information Item III-A

December 9, 2021

Annual Board Audit Awareness Training

Washington Metropolitan Area Transit Authority

Board Action/Information Summary

○ Action ◉ Information	MEAD Number: 202324	Resolution: ○ Yes ◉ No

TITLE:

Annual Audit Awareness Training

PRESENTATION SUMMARY:

Staff will facilitate audit awareness training on Board oversight responsibilities for internal controls.

PURPOSE:

Provide Board Members with annual training on internal controls with a specific focus on Board oversight responsibilities. The training session will fulfill the Board's audit awareness training requirement.

DESCRIPTION:

-

Key Highlights:

The training is designed to increase awareness of internal controls through a discussion of fundamental concepts and current regulatory requirements for internal controls applicable to WMATA. The session will center on a discussion of the Committee of Sponsoring Organizations (COSO's) Internal Control-Integrated Framework and its guidance on Board oversight responsibilities.

The session will also cover risk management as a part of a strong internal control environment using information from the COSO framework - Enterprise Risk Management - Integrating with Strategy and Performance.

Background and History:

Under the direction of the Executive Committee, the training is designed to meet the audit awareness training requirement for new Board Members and serves as a refresher training for existing Members.

The training session will be facilitated by WMATA's office of Management Audits, Risk and Compliance (MARC). MARC is WMATA's Internal Audit Function and provides professional, unbiased, and objective internal audits,

reviews, and assessments of the system of internal controls and related business processes. Audits, reviews, and assessments are designed to add value and improve WMATA's operations. In addition to providing internal audit services, MARC is also responsible for facilitating Enterprise Risk Management (ERM) across the organization with an emphasis on proactive management of risks to strategic, operational, financial, and compliance objectives. In support of its mission, MARC provides regulatory compliance oversight and facilitates organization-wide training on internal controls, risk management, and compliance.

MARC also serves as management's liaison to WMATA OIG on audit matters.

Discussion:

Internal Control - Definition

Internal control is a process, effected by an entity's Board of Directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.

Source: Committee of Sponsoring Organizations of the Treadway Commission (COSO)

Internal Control - Key Concepts

- Geared to the achievement of objectives in one or more categories - operations, reporting, and compliance.
- A process consisting of ongoing tasks and activities - a means to an end, not an end in itself.
- Effected by people - not merely about policy and procedure manuals, systems, and forms, but about people and the actions they take at every level of an organization.
- Able to provide reasonable assurance - but not absolute assurance, to an entity's senior management and Board of Directors.
- Adaptable to the entity structure - flexible in application for the entire entity or a particular subsidiary, division, operating unit, or business process.
- Involves the plans, methods, policies, and procedures that WMATA uses to fulfill its mission, strategic plan, goals, and objectives.
- Internal control is everyone's responsibility.

Internal Control – Value

The achievement of objectives relating to operations, reporting, and compliance:

Operations – Effectiveness and efficiency

Reporting – Internal & external financial & non-financial

Compliance – Adherence to laws and regulations

Internal Control - Standards and Framework

The COSO Internal Control – Integrated Framework (the Framework) outlines the components, principles, and factors necessary for an organization to effectively manage its risks through the implementation of internal controls.

GAO's Green Book – Standards for Internal Control in the Federal Government. The Green Book sets the standards for an effective internal control system for federal agencies and provides the overall framework for designing, implementing, and operating an effective internal control system.

Internal Control - Board Responsibilities

- Establish an oversight structure aligned with the objectives of the organization.
- Establish integrity and ethical values.
- Oversee the definition of and apply the standards of conduct of the organization.
- Develop expectations of competence for organization members.
- Maintain accountability to all members of the oversight body and key stakeholders.
- Commission oversight effectiveness reviews and address opportunities for improvement.
- Oversee management's assessment of risks to the achievement of objectives.
- Evaluate the potential impact of significant changes, fraud, and management override of Internal Control.
- Consider internal and external factors that pose significant risks to the achievement of objectives.
- Determine how proactively the organization manages innovations and changes, such as those triggered by new technology or budgetary and political shifts.
- Provide oversight to management in the development and performance of control activities.
- Make specific inquiries of management regarding the selection, development, and deployment of control activities in significant risk areas and remediation as necessary.
- Communicate direction and tone at the top.
- Obtain, analyze, and discuss information relating to the organization's achievement of objectives
- Review disclosures to external stakeholders for completeness, relevance, and accuracy.
- Allow for and address upward communication of issues

- Assess and oversee the nature and scope of monitoring activities, any management overrides of controls, and management's evaluation and remediation of deficiencies.
- Evaluate the integrity and ethical values of senior management.
- Engage with management, internal and external auditors, and others to evaluate the level of awareness of the organization's strategies, objectives, risks, and control implications associated with the evolving mission, infrastructure, regulations, and other factors.

Risk Management - Key Concepts

- Every entity – whether for-profit, not-for-profit or governmental – exists to provide value for its stakeholders. All entities face risk in the pursuit of value.
- Risk is the possibility that events will occur and affect the achievement of strategy and business objectives, which may be positive or negative.
- Risk management includes identifying, assessing, monitoring, and responding to risks.
- Enterprise Risk Management is the process that allows organizations to identify, evaluate, and manage risks that could significantly disrupt the successful achievement of mission and objectives.
- Management holds primary responsibility for managing risks.
- The Board has an oversight role for risk across the organization.

Board Responsibilities for Risk Management

- Understand the strategy, operating model, industry, and issues and challenges affecting the organization.
- Assess the appropriateness of the organization's strategy, alignment to the mission, vision, and core values, and the risk inherent in that strategy.
- Oversee management assessment of risks to the achievement of objectives.
- Review and understand the most significant risks, including emerging risks, and significant changes in the portfolio view of risk, including management responses and actions.
- Review, approve, challenge, and concur with management on proposed strategy and risk appetite.
- Assess internal and external information and insights conductive to effective risk oversight.
- Obtain input from internal and external auditors, and other independent parties regarding management perceptions and assumptions related to risk.

Roles and Responsibilities for Risk and Controls Illustrated – The Three Lines Model

Everyone at WMATA has some responsibility for internal control. To help ensure that organizational objectives are achieved, and essential duties are performed as intended, the Three Lines Model clarifies specific roles and

responsibilities. The Model aims to enable value creation and value protection, as well as the overall accomplishment of the organization's mission and objectives. A responsible body (the Board or Board equivalent and its various committees) is needed to provide governance and oversight.
Management executes and manages processes and activities that accomplish the objectives, which includes management control as the First Line and risk and control monitoring arms of management as the Second Line. To ensure value creation and protection, Internal Audit provides independent assurance to verify that processes and activities are being completed as expected and to identify opportunities for improvement where applicable. Internal Audit is the Third Line in this model.

Note: See Board training presentation for an illustration of the Three Lines Model.

FUNDING IMPACT:

Define current or potential funding impact, including source of reimbursable funds.	
Project Manager:	Elizabeth Sullivan,Vice President, Chief Risk and Audit Officer
Project Department/Office:	Management Audits, Risk and Compliance (MARC)

TIMELINE:

Previous Actions	Last Annual Board Audit Awareness Training was on 12/10/2020.
Anticipated actions after presentation	N/A

RECOMMENDATION:

-

Annual Audit Awareness Training

Oversight Responsibilities for Internal Controls

Executive Committee

December 9, 2021

Elizabeth Sullivan, VP Chief Risk and Audit Officer
Management Audits, Risk and Compliance

Purpose

Training Objectives

- Increase awareness of Internal Controls
- Discuss Board of Directors oversight responsibilities

Introduction to MARC

Management Audits, Risk and Compliance (MARC) Internal Audit	WMATA OIG Office of Audits
• Reports to WMATA's General Manager/Chief Executive Officer	• Reports to WMATA's Board of Directors
• Independent from the processes, Offices and Departments it evaluates	• Independent from WMATA management
• Provides independent assurance to management, and reports information to the Board as applicable	• Provides independent assurance to the public, Board, management, and external stakeholders
• Focuses on internal compliance and oversight with an emphasis on proactive management of risks to WMATA's strategic, operational, financial, and compliance objectives to promote efficiency and effectiveness of operations	• Focuses on promoting economy, efficiency, and effectiveness, as well as preventing and detecting fraud, waste, and abuse
• Acts as a liaison to external auditors and reviewers, including WMATA OIG, and independently tracks and monitors WMATA's corrective actions, including actions in response to financial statement audits	• Oversees the independent audit of financial statements

Internal Control — Definition and Key Concepts

Internal control is a process, effected by an entity's Board of Directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance

Source: Committee of Sponsoring Organizations of the Treadway Commission (COSO)

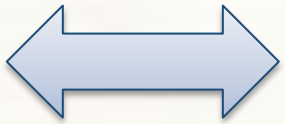
Internal control is everyone's responsibility

Regulatory Expectations

- Section 200.303 Office of Management Budget's (OMB) – Uniform Guidance:
  - Establish and maintain effective internal controls over Federal awards in compliance with:
    - COSO - Internal Control Integrated Framework, or
    - Green Book - Standards for Internal Control in the Federal Government

- FTA Circular 5010 (FTA C 5010.1E Chapter VI §2) – Establish and maintain adequate Internal Controls

Internal Control - Standards and Framework



COSO — Control Environment

Foundation for all other components of Internal Control

1. Demonstrates commitment to integrity and ethical values
2. Exercises oversight responsibility
3. Establishes structure, authority and responsibility
4. Demonstrates commitment to competence
5. Enforces accountability

Control Environment — Board Responsibility

- Establish oversight structure aligned with objectives of organization
- Establish integrity and ethical values
- Oversee the definition of and apply the standards of conduct of the organization
- Develop expectations of competence for organization members
- Maintain accountability to all members of the oversight body and key stakeholders
- Commission oversight effectiveness reviews and address opportunities for improvement

COSO — Risk Assessment

Identification and analysis of relevant risks to the achievement of objectives

6. Specifies suitable objectives
7. Identifies and analyzes risk
8. Assesses fraud risk
9. Identifies and analyzes significant change

Risk Assessment – Board Responsibility

- Oversee management's assessment of risks to the achievement of objectives
- Evaluate the potential impact of significant changes, fraud, and management override of Internal Control
- Consider internal and external factors that pose significant risks to the achievement of objectives
- Determine how proactively the organization manages innovations and changes such as those triggered by new technology or budgetary and political shifts

COSO — Control Activities

Policies and procedures which help ensure that management directives are carried out

10. Selects and develops control activities
11. Selects and develops general controls over technology
12. Deploys through policies and procedures

Control Activities – Board Responsibility

- Provide oversight to management in the development and performance of control activities
- Make specific inquiries of management regarding the selection, development, and deployment of control activities in significant risk areas and remediation as necessary

COSO — Information and Communication

4

Information and Communication

Identification, capture and communication of data and pertinent business information in a form and timeframe that enables people to carry out their responsibilities

13. Uses relevant information
14. Communicates internally
15. Communicates externally

Information & Communication – Board Responsibility

- Communicate direction and tone at the top
- Obtain, analyze, and discuss information relating to the organization's achievement of objectives
- Review disclosures to external stakeholders for completeness, relevance, and accuracy
- Allow for and address upward communication of issues

COSO — Monitoring Activities

Helps ensure that Internal Controls continue to operate effectively and involves assessment by appropriate personnel

16. Conducts ongoing and/or separate evaluations
17. Evaluates and communicates deficiencies

Monitoring Activities – Board Responsibility

- Assess and oversee:
  - Nature and scope of monitoring activities
  - Management overrides of controls
  - Management's evaluation and remediation of deficiencies
- Evaluate the integrity and ethical values of senior management
- Engage with management, internal and external auditors, and others to:
  - Evaluate the level of awareness of the organization's strategies, objectives, risks, and controls
  - Understand the implications associated with evolving mission, infrastructure, regulations, and other factors

Risk Management

The Premise

Every entity – whether for profit, not-for-profit, or governmental – exists to provide value for its stakeholders. All entities face risk in the pursuit of value.

Risk is the possibility that events will occur and affect the achievement of strategy and business objectives, which may be positive or negative.

Enterprise Risk Management

The process that allows organizations to identify, evaluate, and manage risks that could significantly disrupt the successful achievement of mission and objectives. (AFERM)

The culture, capabilities, and practices, integrated with strategy-setting and its performance, that organizations rely on to manage risk in creating, preserving, and realizing value. (COSO ERM)

Coordinated activities to direct and control an organization with regard to risk. (ISO 31000, International Standards Organization)

Risk Management – Why Important?

- Successful organizations have a culture of risk management
- Improves decision-making and supports the deployment of resources based on risk
- Encourages open communications about significant risks and reduces gaps and inconsistencies with the management of process level objectives
- Enhances knowledge management and workforce development
- Mature transit agencies and other progressive organizations have an explicit risk management structure

Enterprise Risk Management Program - Overview

Risk assessment is an iterative process that occurs enterprise-wide and considers risk across all levels of the organization.

COSO Assess Risks Process Flow Diagram

Risk Assessment Approach

Entity Level Risks

Entity Level Risks have the most pervasive (significant) impact on the accomplishment of WMATA's mission, vision, core values, selected strategies, and related goals and objectives.

Process Level Risks

These are risks that emanate from business processes, which are a collection of related and structured activities or actions that support the achievement of core business objectives typically defined at the Department or Office level.

Special Focus Risks

Risks from a special focus activity or potential risk exposure that ascends to special focus due to management concern, special interest, or event-driven. i.e., Fraud Risk, Project Risk, Vendor Risk, etc.

Risk Management Framework and Principles

Governance & Culture

1. Exercises Board Risk Oversight
2. Establishes Operating Structures
3. Defines Desired Culture
4. Demonstrates Commitment to Core Values
5. Attracts, Develops, and Retains Capable Individuals

Strategy & Objective-Setting

6. Analyzes Business Context
7. Defines Risk Appetite
8. Evaluates Alternative Strategies
9. Formulates Business Objectives

Performance

10. Identifies Risk
11. Assesses Severity of Risk
12. Prioritizes Risks
13. Implements Risk Responses
14. Develops Portfolio View

Review & Revision

15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues improvement in Enterprise Risk Management

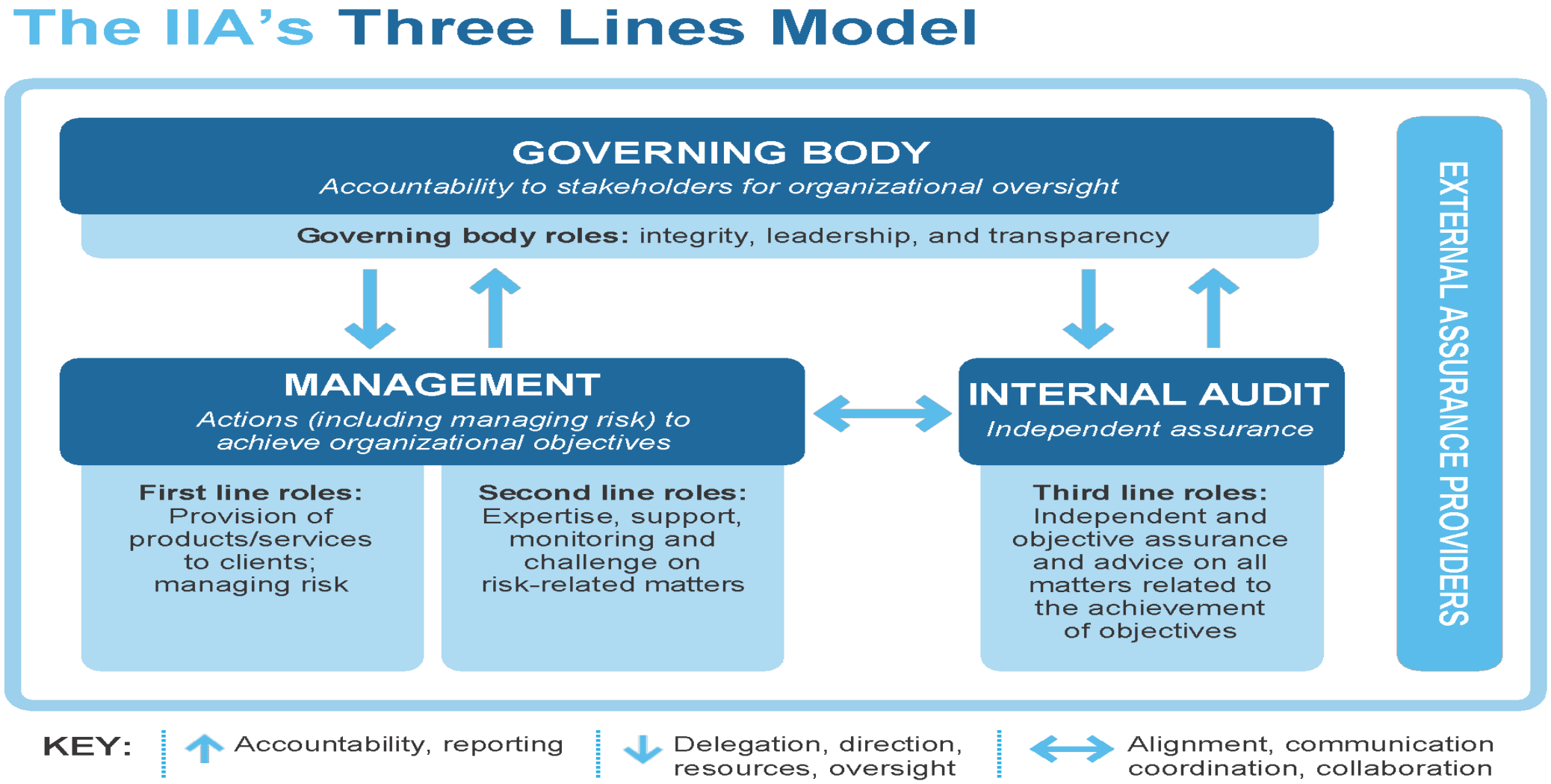
Information, Communication, & Reporting

18. Leverages Information and Technology
19. Communicates Risk Information
20. Reports on Risk, Culture, and Performance

Source: Committee of Sponsoring Organizations of the Treadway Commission (COSO) – Enterprise Risk Management Framework

Board Oversight Responsibility

Roles and Responsibilities for Risk and Controls Illustrated



Source: The Institute of Internal Auditors

Session Summary

- Management of risk and internal controls are important to the success of any organization
- Board has oversight responsibilities for risk and internal controls
- Responsibilities include, commissioning oversight reviews, evaluating impact of change, making specific inquiries of management, communicating direction and tone at the top, obtaining and analyzing relevant information, and overseeing monitoring activities
- Management has the first line responsibility for risk and controls
- Communication is key to an effective risk management process