Executive Committee

Information Item III-C

November 21, 2024

Annual Audit Awareness Training

Washington Metropolitan Area Transit Authority

Board Action/Information Summary

○ Action ● Information	Document Number: 211877	Resolution: ○ Yes ● No

Presentation Name:

Annual Audit Awareness Training

Project Manager:

Elizabeth Sullivan

Project Department:

Audit and Compliance

Purpose/Key Highlights:

PURPOSE:
Provide the Board with annual training with a specific focus on Board role and responsibilities for Internal Control and Risk Management. The session will fulfill the Board's audit awareness training requirement.

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.

Interested Parties:

There are no interested parties.

Background:

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 the Audit and Compliance department. Audit and Compliance, WMATA's Internal Audit Function, 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 Metro's operations. In addition to providing internal audit services, Audit and Compliance is also responsible for facilitating Enterprise Risk Management (ERM) across the organization emphasizing the proactive management of risks to strategic, operational, financial, and compliance objectives. Audit and Compliance provides regulatory compliance oversight and facilitates organization-wide training on internal controls, risk management, and compliance.

Audit and Compliance also serves as the Authority'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

Every entity – 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 - Definition

The process that allows organizations to identify, evaluate, and manage risks that could significantly disrupt the successful achievement of mission and objectives (Association for Federal Enterprise Risk Management - 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 (The Committee of Sponsoring Organizations - COSO ERM).

Coordinated activities to direct and control an organization with regard to risk (International Organization for Standardization - ISO 31000:2018).

Enterprise Risk Management Program Overview

The ERM Program establishes the standards, processes, and accountability structure to consistently identify, assess, respond to, and monitor significant risk across WMATA.

The program requires that we formally assess risk, at least annually, or in response to a significant change in the business environment – internal and external.
Risk assessment is an iterative process that occurs enterprise-wide, and the management of risk should be a natural part of managing the business.
Risks may arise from different levels of the organization; as such, the ERM program allows for the identification and assessment of risks at multiple levels and across six representative functional areas.

Multiple Levels

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.).

Functional Areas

Safety and Security, Transit, Transit Support Services, Business Support Services, Financial Management, and Technology.

Risk Categories

Risks are aligned to seven Risk Categories to promote a common language to recognize and describe potential risks that can impact the achievement of objectives. The ERM program defines these risk categories based on WMATA's internal and external business context.

Board Responsibilities for Risk Management

- Oversee management's assessment of risks to the achievement of objectives.
- Review, approve, challenge, and concur with management on proposed strategy and risk appetite.
- 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.
- Review and understand the most significant risks, including emerging risks, and significant changes in the portfolio view of risk, including management responses and actions.
- 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 evolving mission, infrastructure, regulations, and other factors.

Funding Impact:

No impact on funding.

Previous Actions:

Last Annual Board Audit Awareness Training - 11/02/2023

Next Steps:

Annual Audit Awareness Training - Fall 2025

Recommendation:

Information Only

Washington Metropolitan
Area Transit Authority

November 21, 2024

Annual Board Audit Awareness Training

Executive Committee

Your Metro, the Way Forward

Service excellence
Deliver safe, reliable, convenient, equitable, accessible, and enjoyable service for customers.

Talented teams
Attract, develop, and retain top talent where individuals feel valued, supported, and proud of their contribution.

Regional opportunity & partnership
Design transit service to move more people and equitably connect a growing region.

Sustainability
Manage resources responsibly to achieve a sustainable operating, capital, and environmental model.

Sound **Internal Controls** and **Risk Management** practices provide reasonable assurance that Metro goals and objectives will be met.

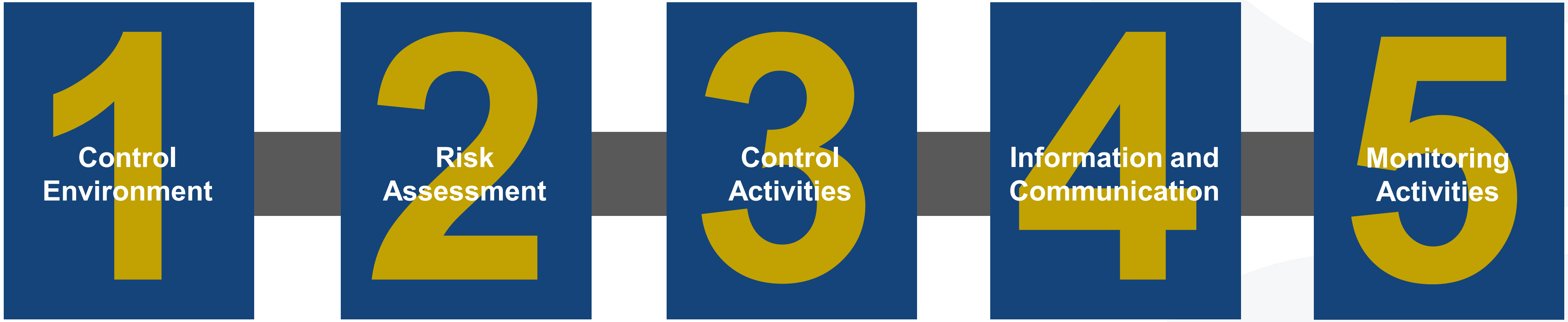
While management is responsible for maintaining a strong internal control environment and employing appropriate risk management practices, the Board has an oversight role for risks and internal controls.

Agenda

- Board Oversight Responsibility:
  - Internal Controls
  - Risk Management

Committee of Sponsoring Organizations (COSO's) Internal Control-Integrated Framework

Internal control consists of five integrated components



Foundation for all other components of Internal Control

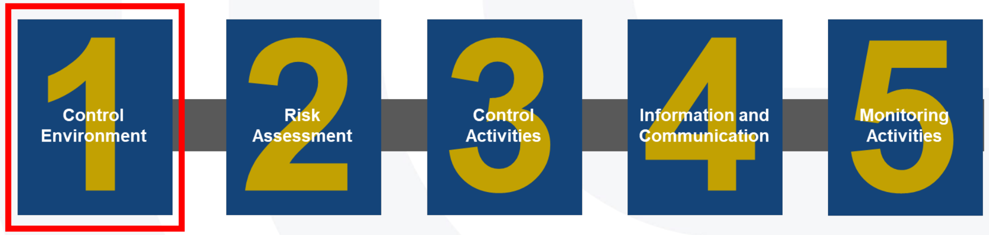
Identification and analysis of relevant risks to the achievement of objectives

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

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

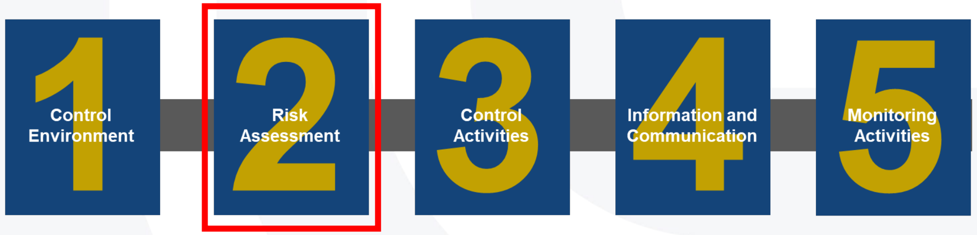
Helps ensure that Internal Controls continue to operate effectively and involves assessment by appropriate personnel

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

Risk Assessment —
Board Responsibility



1 Control Environment

2 Risk Assessment

3 Control Activities

4 Information and Communication

5 Monitoring Activities

- 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

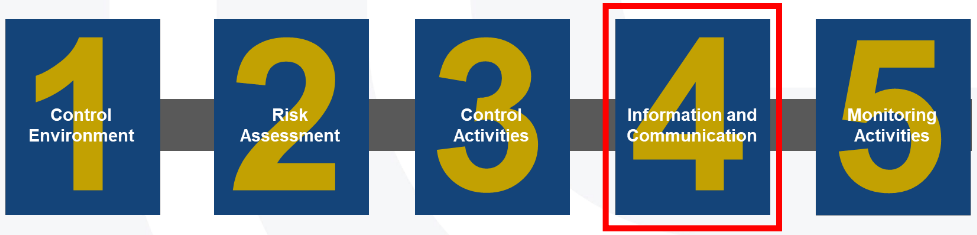
Control Activities —

Board Responsibility

1
Control Environment
2
Risk Assessment
3
Control Activities
4
Information and Communication
5
Monitoring Activities

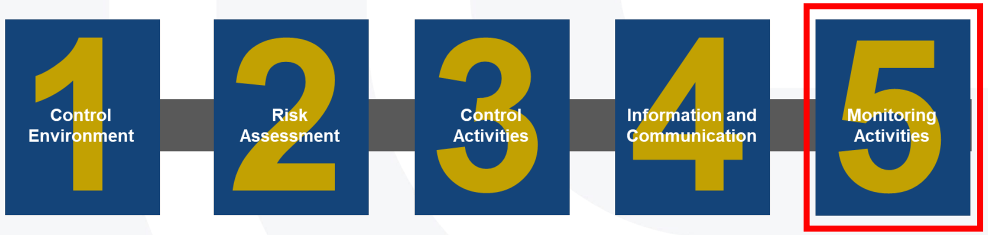
- Provide oversight to management in the development and performance of control activities
- Make specific inquiries of management regarding the selection, development, and deployment of control activities in significant risk areas and remediation as necessary

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

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

Why is Risk Management Important?

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

Definition of Risk

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.
- 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.

Enterprise Risk Management Program Overview

- Formally assess risk, at least annually, or in response to a significant change in the business
- An iterative process that occurs enterprise-wide, and should be a natural part of managing business
- Risks may arise from different levels of the organization; as such, the Metro ERM program allows for the identification and assessment of risks at various levels:

  Entity Level – most pervasive impact on Metro’s mission

  Process Level – business process and activities within each Metro Department and Office

  Special Focus Level – special focus activity or potential risk exposure that ascends to special focus

- Identified across six functional areas

Safety and Security

Transit

Transit Support Services

Business Support Services

Financial Management

Technology

Risk Management

Board Responsibility

- Oversee management’s assessment of risks
- Review, approve, challenge, and concur with management on proposed strategy and risk appetite
- Consider internal and external factors that pose significant risks
- Determine how proactively the organization manages innovation and change
- Review and understand the most significant risks, including emerging risks, and management responses and actions
- Engage with management and internal and external assurance providers

Risk Landscape — Transit Perspective

Top Risks for Transit

- Cybersecurity
- Human Capital
- Digital Disruption, Including AI
- Supply Chain and Outsourcing
- Regulatory Changes
- Financial Liquidity
- Business Continuity
- Communication and Reputation
- Market Changes
- Geopolitical Uncertainty
- Safety and Security
- Transit Asset Management & Reliability

Metro Risk Watch

- Funding Unpredictable & Not Sustainable
- Cybersecurity
- Public Safety
- Policies, Procedures & Compliance
- Transit Asset Management & Reliability
- Third Party & Vendor Management
- External Threats & Emergency Preparedness
- Reputation & Stakeholder Perception
- Digital Innovation & Evolving Technology (Digital Disruption – Including AI)
- Human Capital & Diversity, Equity & Inclusion

Top Risk for transit as discussed by the American Public Transportation Association (APTA's) Committee of Audit Professionals November 2024. Preliminary as of 11/12/2024.

🟦 Risk noted by Metro's ERM Program