



Executive Committee

Board Information Item III-B

December 8, 2022

Annual Audit Awareness Training

Washington Metropolitan Area Transit Authority
Board Action/Information Summary

☐ Action ☒ Information

MEAD Number:
203414

Resolution:
☐ Yes ☒ No

TITLE:

Annual Audit Awareness Training

PRESENTATION SUMMARY:

Staff will facilitate audit awareness training on Board role and responsibilities for Enterprise Risk Management.

PURPOSE:

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

DESCRIPTION:

The training raises awareness of Enterprise Risk Management (ERM) through a discussion of fundamental concepts such as the definition and benefits of ERM and an overview of Metro's Enterprise Risk Management Program.

Key Highlights:

The discussion will be based on the framework that guides Metro's ERM program, the Committee of Sponsoring Organizations (COSO) ERM Framework - Enterprise Risk Management – Integrating with Strategy and Performance, and its guidance on Board role and responsibilities for Enterprise Risk Management.

The session will also cover the importance of risk management as a part of a strong internal control environment.

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 Metro'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 Metro's operations. In addition to providing internal audit services, MARC 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. MARC also provides regulatory compliance oversight and facilitates organization-wide training on internal controls, risk management, and compliance.

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

Discussion:

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).

Benefits of Enterprise Risk Management

- Successful organizations have a culture of risk management
- Improves decision-making and supports the deployment of resources
- 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

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



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 Metro's 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 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 Metro'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 Metro 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 Operations, Transit Support Services, Business Support Services, Financial Management, and Technology.

Risk Categories

Risks are aligned to eight 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 Metro's internal and external business context as summarized below.

	Financial Management	Evaluates risk in terms of Metro's ability to meet its financial obligations. This includes processes related to planning, directing, managing, and controlling financial resources.
	Regulatory Compliance	Evaluates risk in terms of Metro's ability to comply with or a failure to detect and report activities that compliant with applicable external rules and regulations, and internal policies and guidelines.
	Legal	Evaluates risk in scenarios where there is no clear, controlling legal authority or where the law is uns particular issue.
	Reputation	Evaluates risk in terms of internal or external stakeholder opinion. Reputation risk affects Metro's ab establish new and sustain existing relationships.
	Safety and Security	Evaluates risk in terms of Metro's ability to prevent hazards that may cause harm to people, equipm environment.
	Service Delivery	Evaluates risk that may have a direct or indirect impact on daily transit and business operations at M including direct or indirect losses or other negative effects due to inadequate processes and operatic
	Strategic	Evaluates risk in terms of Metro's ability to achieve its strategic or tactical objectives, any adverse bu decision, or a lack of strategic direction and leadership.
	Technology	Evaluates risk associated with the inability of networks, security, and other technologies to meet Met evolving needs, and its mission, goals and objectives.

Highlights of Metro ERM Framework and Policy and Risk Management – Key Concepts

Policy Highlights

- Built on the foundational elements of an established framework – COSO ERM – Enterprise Risk Management – Integrating With Strategy and Performance
- Outlines a methodology, process, and approach
- Acknowledges the diverse nature of the portfolio of risks facing a complex organization
- Defines general risk-taking guidelines and risk performance measures

Risk Management Concepts

Risk Management – Includes identifying, assessing, monitoring, and responding to risks.

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.

Management – Has the primary responsibility for managing risks.

Board of Directors – Have an oversight role for risk across the organization.

Risk Capacity – The maximum amount of risk that Metro can absorb in pursuit of a strategy of business objectives. It is Metro's policy not to exceed the organization's risk capacity.

Risk Appetite – Risk appetite is the type and amount of risk on a broad level that Metro is willing to accept in pursuit of business objectives. The risk appetite considers the level of risk that management consciously accepts after balancing the cost and benefits of implementing key controls.

Target Risk Appetite – The Amount of risk desired or an optimum level of risk.

Risk Tolerance – The boundaries of acceptable variation relative to the achievement of objectives, which must align with Metro's risk appetite.

Expressing Risk Appetite

Why Create a Risk Appetite Statement?

- Formalize the way Metro expresses the risk taken and reflect philosophy on risk-taking.
- Set the general, high-level boundaries within which Metro desires to operate.
- Empower management to make risk-based decisions given the nature and type of risk and provide a decision-making tool to guide management.

Approach to Developing Risk Appetite

- Risk appetite may be articulated in the context of objectives that align to mission, vision, core values, business objective categories, and performance targets.
- Risk appetite may also be expressed as a continuum.

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:

Define current or potential funding impact, including source of reimbursable funds.	
Project Manager:	Elizabeth Sullivan
Project Department/Office:	Office of Management Audits, Risk and Compliance

TIMELINE:

Previous Actions	Annual Board Audit Awareness Training - 12/09/2021
Anticipated actions after presentation	Board Audit Awareness Training Planned for 2023

RECOMMENDATION:

-

Annual Board Audit Awareness Training

Enterprise Risk Management
Board Role and Responsibility

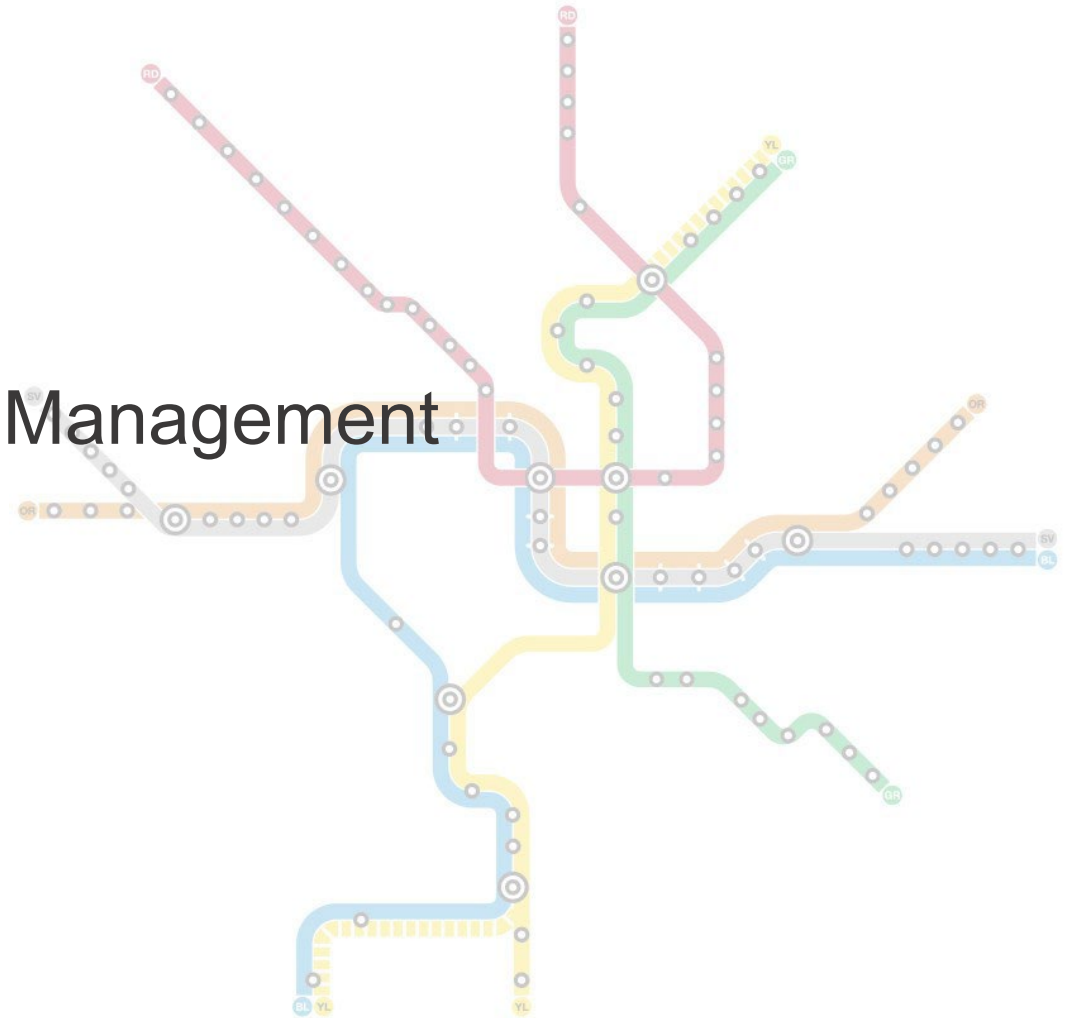
Elizabeth Sullivan
VP, Chief Risk and Audit Officer
December 8, 2022



Purpose

Training Objectives

- Increase awareness of Enterprise Risk Management
- Discuss Board role and responsibilities



Board Role and Responsibility

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

1. The process that allows organizations to identify, evaluate, and manage risks that could significantly disrupt the successful achievement of mission and objectives. (AFERM)
2. 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)
3. Coordinated activities to direct and control an organization with regard to risk. (ISO 31000, International Standards Organization)

Board Role and Responsibility

Benefits of Risk Management

Successful organizations have a culture of risk management



Improves decision-making and supports the deployment of resources



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

Board Role and Responsibility

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
Operations

Transit
Support
Services

Business
Support
Services

Financial
Management

Technology

Board Role and Responsibility

Enterprise Risk Management Program Overview

1. Identify - Identification and analysis
2. Assess - Assess severity though impact and probability of occurrence
3. Respond - Accept, Avoid, **Mitigate**, Share, Enhance or Explore
4. Monitor - Ongoing monitoring and reporting



Board Role and Responsibility

Risks are aligned to Eight Risk Categories



**Financial
Management**



**Regulatory
Compliance**



Legal



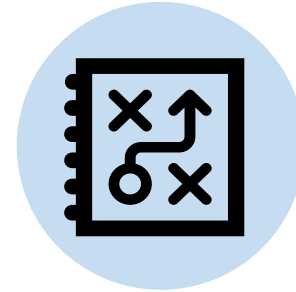
Reputation



**Safety and
Security**



**Service
Delivery**



Strategic



Technology

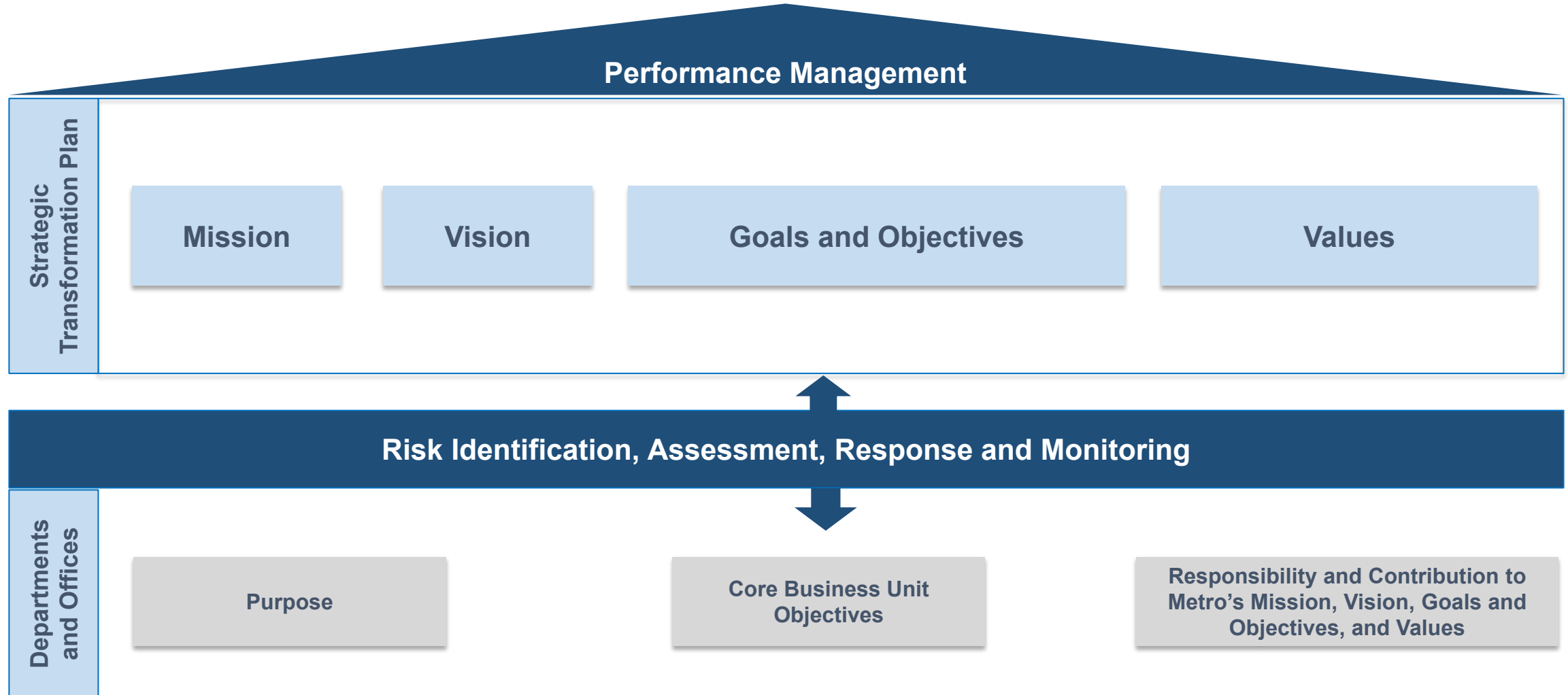
Board Role and Responsibility

ERM Framework and Internal Control Policy Highlights

- Built on the foundational elements of an established framework – COSO ERM – *Enterprise Risk Management – Integrating With Strategy and Performance*
- Defines Risk Governance – Board and Management Roles and Responsibilities
- Outlines a methodology, process, and approach
- Acknowledges the diverse nature of the portfolio of risks facing a complex organization
- Defines general risk-taking guidelines and risk performance measures
- Defines Risk Appetite inherent in Metro's mission
- Requires the development of *Risk Registers* for each Department and *Risk Profiles & Risk Portfolios* necessary for the appropriate analysis of risks facing Metro
- Requires data-informed risk management and the identification and monitoring of Key Risk Indicators (KRI)

Board Role and Responsibility

ERM Framework outlines expectations to ***Integrate Risk Management, Strategy, and Performance***




Board Role and Responsibility

Why Create a Risk Appetite Statement?

- Reflects philosophy on risk-taking
- Sets boundaries within which Metro desires to operate
- Empowers management to make risk-based decisions

Approach to Developing Risk Appetite

- Articulated in the context of objectives that align with the mission, vision, core values, business objective categories, or performance targets
- Expressed as a continuum

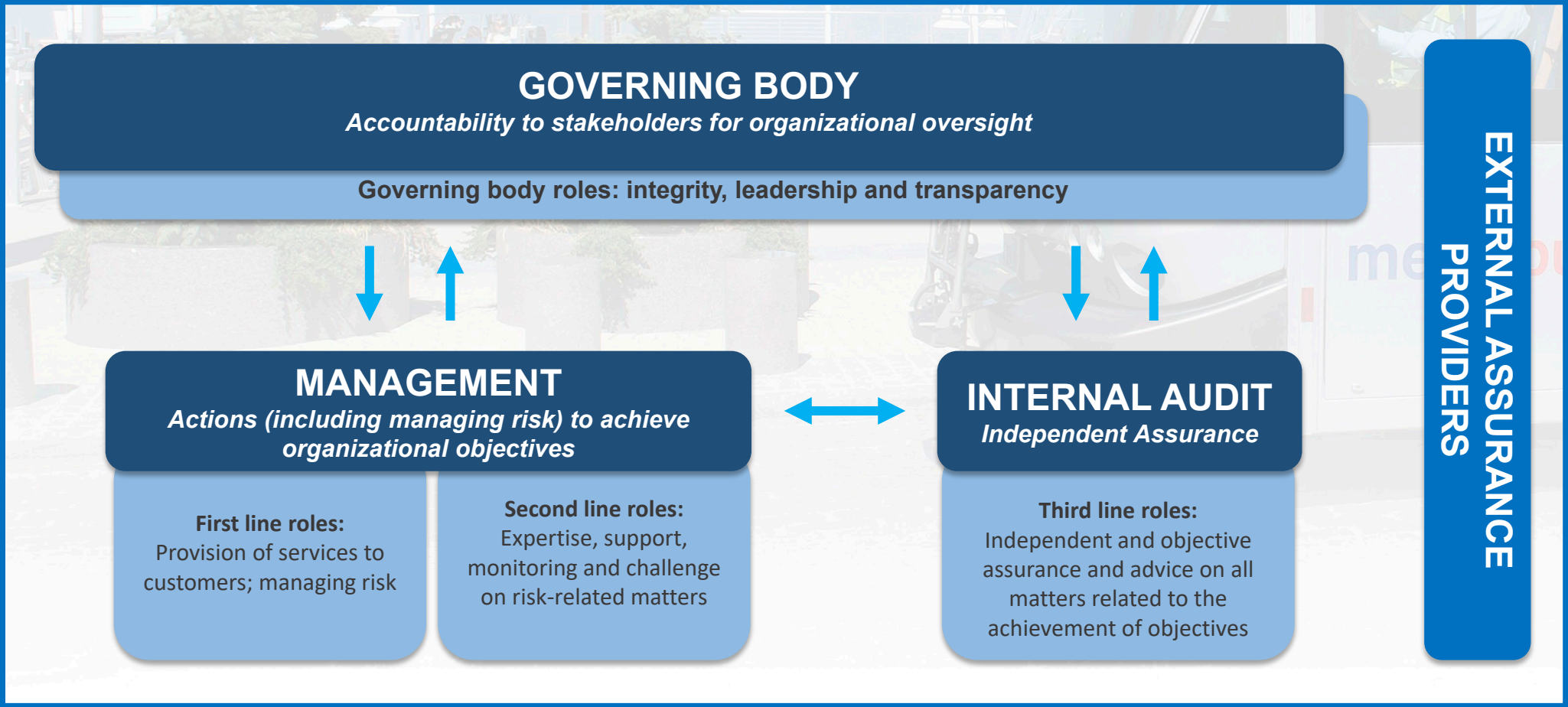


Lower appetite for risks that impact safety & regulatory compliance expectations

Higher appetite for risks that create value through creative innovation

Board Role and Responsibility

Illustration of Roles and Responsibilities for Risk Management



KEY: Accountability, reporting Delegation, direction, resources, oversight Alignment, communication, coordination, collaboration

Source: The Institute of Internal Auditors
Illustrated for Metro



Board Oversight Responsibility

Board Roles and Responsibilities for Risk Management

- 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

Board Role and Responsibility

Are you asking the right questions about



The Board should **Review**, **Challenge**, and **Concur** with management on:

- Proposed strategy and risk appetite
- Alignment of strategy and business objectives with Metro's stated mission, vision, and core values
- Significant business decisions, including capital allocations, funding, and other decisions
- Response to significant fluctuations in performance or the portfolio view of risk
- Response to instances of deviation from core values

Board Role and Responsibility

Top 10 Risks for Transit in 2022

1. Talent Management
2. Ridership Uncertainty
3. Cybersecurity
4. Data Governance
5. Organizational Governance
6. Third Party
7. Sustainability
8. Economic and Political Volatility
9. Disruptive Innovation
10. Capital Program Delivery



Top risk for transit as discussed by the American Public Transportation Association (APTA's) Committee of Audit Professionals – August 2022

■ Top risk noted by Metro's ERM Program as of July 2022

Board Role and Responsibility

Session Summary

- Managing risk is important to the success of any organization
- Board has oversight responsibilities
- Board should review, challenge, and concur with management on proposed strategy and risk appetite, and alignment of strategy and business objectives with Metro's mission, vision, and values
- Board should evaluate the impact of change, make specific inquiries of management, communicate direction and tone at the top, obtain and analyze relevant information, and oversee monitoring activities
- Management has the primary responsibility for managing risk
- Communication is key to an effective risk management process