



**Executive Committee**

**Information Item III-B**

**November 2, 2023**

## **Annual Audit Awareness Training**

Washington Metropolitan Area Transit Authority

## Board Action/Information Summary

☐ Action ☒ Information

Document  
Number:  
205628

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 training 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. It 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 WMATA's operations.

In addition to providing internal audit services, Audit and Compliance:

- Facilitates Enterprise Risk Management (ERM) across the organization emphasizing the proactive management of risks to strategic, operational, financial, and compliance objectives.
- Provides regulatory compliance oversight and facilitates organization-wide training on internal controls, risk management, and compliance.
- 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.

## **Board Responsibilities for Internal Control**

- 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).

### 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.

## **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:**

There is no impact to funding for this training.

**Previous Actions:**

Last Annual Board Audit Awareness Training - 12/08/2022

**Next Steps:**

Annual Audit Awareness training - Fall 2024

**Recommendation:**

Information Only



# Annual Board Audit Awareness Training

Internal Controls and Risk Management  
Board Role and Responsibility

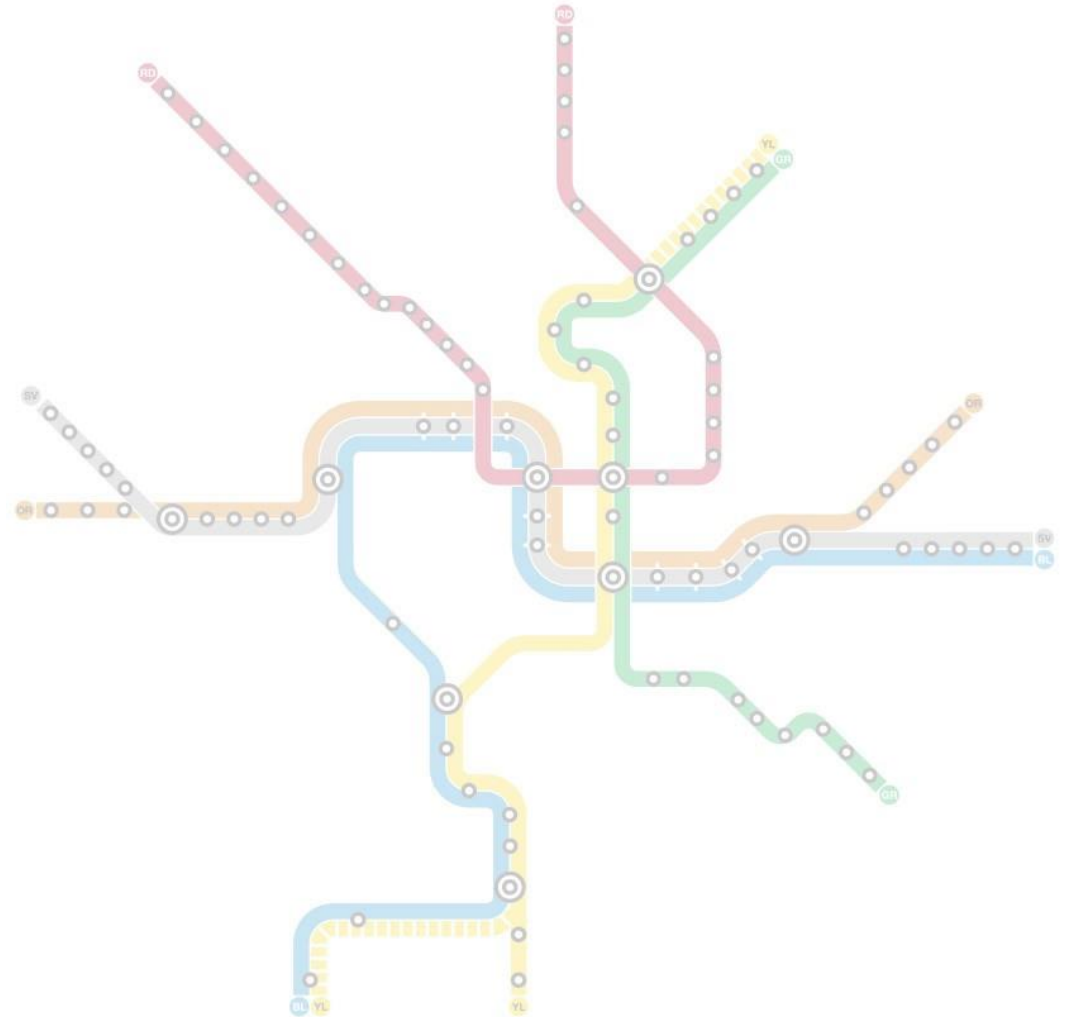
Executive Committee  
November 2, 2023



# Purpose

## Training Objectives

- Increase awareness of Internal Controls and Risk Management
- Discuss Board role and responsibilities



# 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**

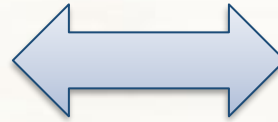
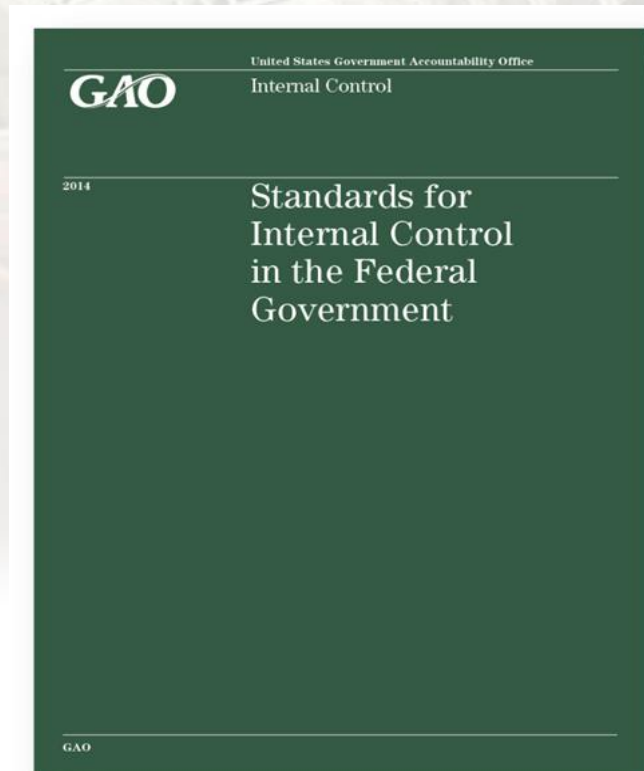
# Regulatory Expectations



- 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



## 1 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



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

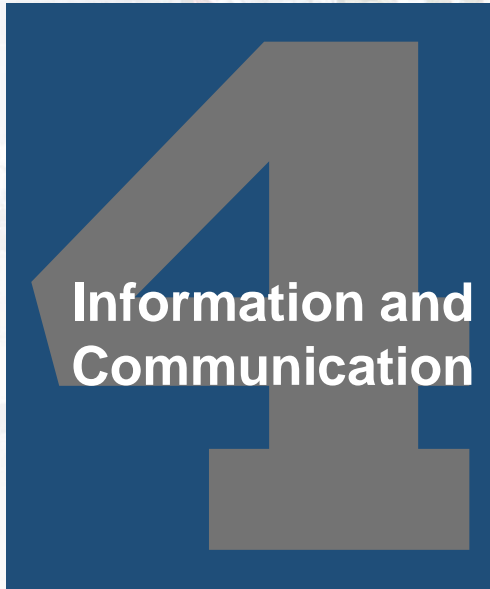


Policies and procedures which help ensure that management directives are carried out

- 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



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



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

# Board Role and Responsibility

## 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

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. (International Organization for Standardization - ISO 31000:2018)



# 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

## 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

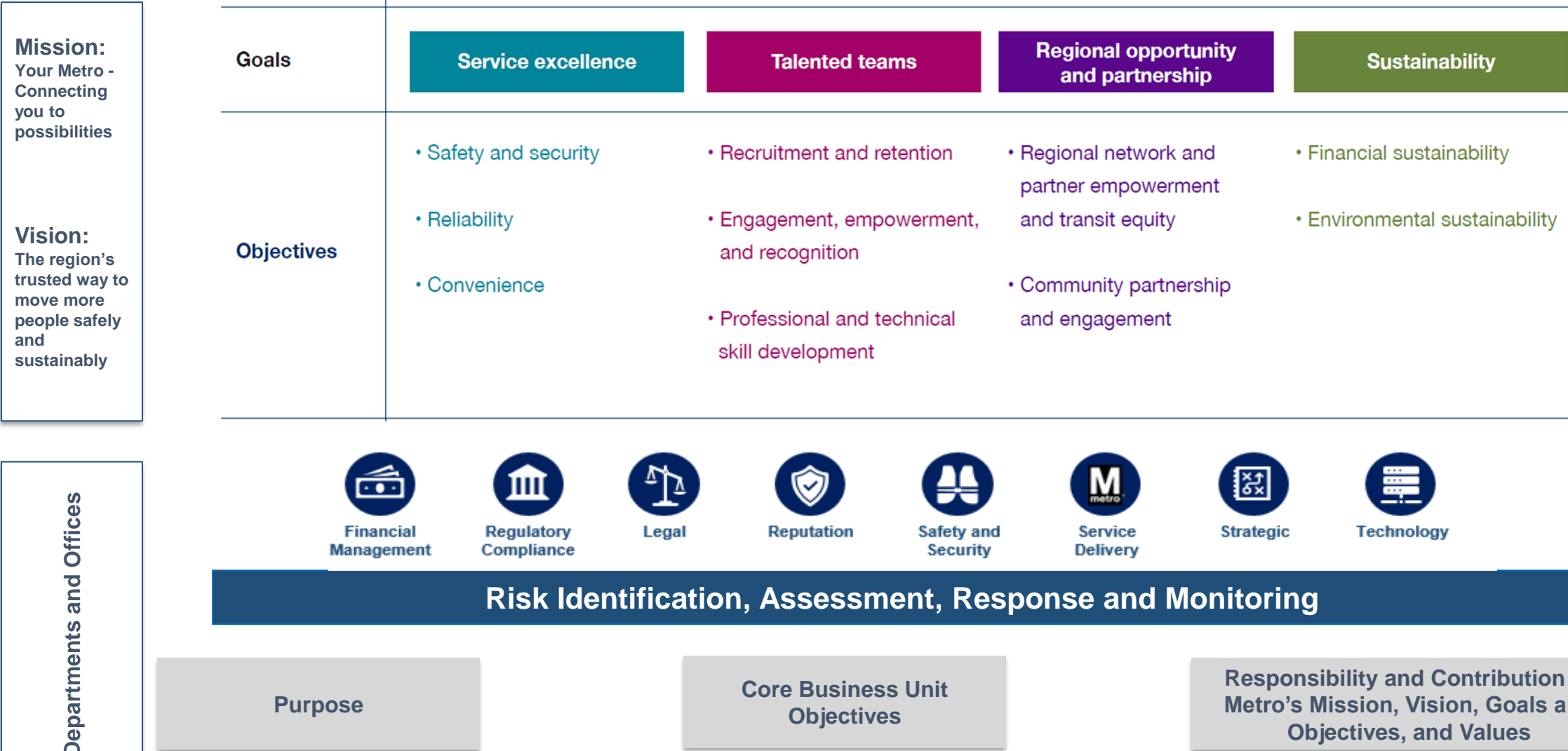
Transit  
Support  
Services

Business  
Support  
Services

Financial  
Management

Technology

## Risks to Strategic Plan Goals & Objectives



## 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

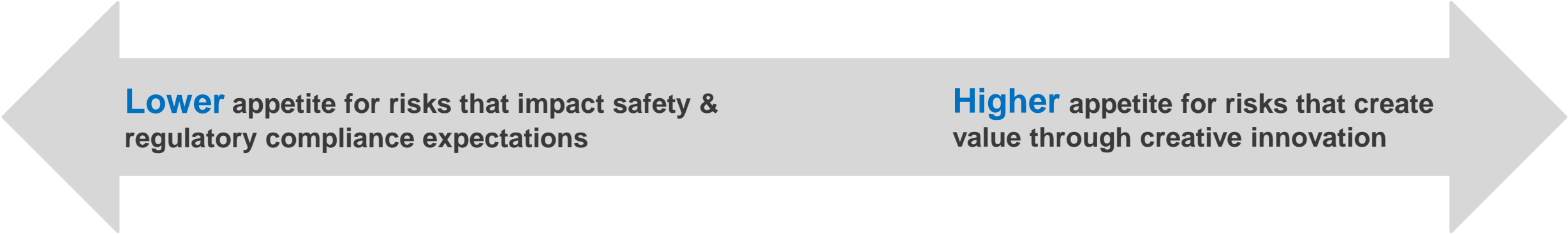
# Board Role and Responsibility

## 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

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

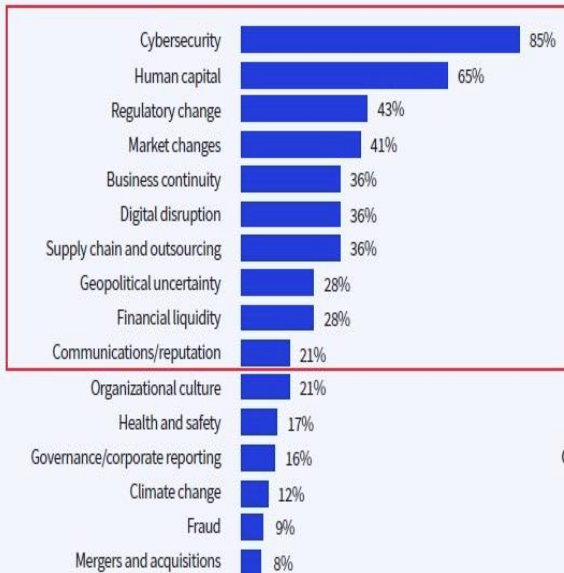
## Risk Landscape - North American Perspective

■ Cybersecurity and human capital dominated the risk landscape for North America for 2024.

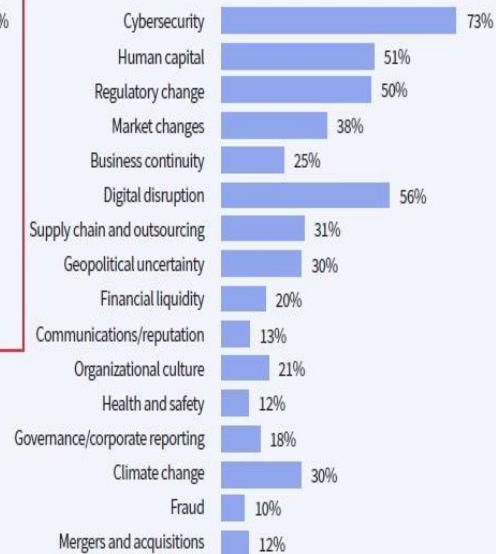
■ In the next 3 years, digital disruption and climate change are the risks expected to increase the most.

■ Current risk  
■ Future risk

What are the top 5 risks your organization currently faces?



What are the top 5 risks your organization will face 3 years from now?



### Risk in Focus 2024 Risk Categories

Risk Topic	Risk Description Used in the Survey
Business continuity	Business continuity, operational resilience, crisis management, and disaster response
Climate change	Climate change, biodiversity, and environmental sustainability
Communications/reputation	Communications, reputation, and stakeholder relationships
Cybersecurity	Cybersecurity and data security
Digital disruption	Digital disruption, new technology, and AI
Financial liquidity	Financial, liquidity, and insolvency risks
Fraud	Fraud, bribery, and the criminal exploitation of disruption
Geopolitical uncertainty	Macroeconomic and geopolitical uncertainty
Governance/corporate reporting	Organizational governance and corporate reporting
Health and safety	Health, safety, and security
Human capital	Human capital, diversity, and talent management and retention
Market changes	Market changes/competition and customer behavior
Mergers and acquisitions	Mergers and acquisitions
Organizational culture	Organizational culture
Regulatory change	Change in laws and regulations
Supply chain and outsourcing	Supply chain, outsourcing, and 'nth' party risk

Source: The Internal Audit Foundation's Risk in Focus 2024 Report Series. Risk in Focus provides practical, data-driven research to help internal auditors and their stakeholders understand today's risk environment and prepare audit plans for the year ahead.

[Risk in Focus \(theiaa.org\)](https://theiaa.org/risk-in-focus)

## 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
- 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
- Management has the first line responsibility for risk and controls
- Communication is key to an effective risk management process