Executive Committee

Information Item II-A

December 13, 2018

Annual Audit Awareness Training

Washington Metropolitan Area Transit Authority

Board Action/Information Summary

○ Action ● Information	MEAD Number: 202050	Resolution: ○ Yes ● No

TITLE:

Board Audit Awareness Training

PRESENTATION SUMMARY:

The 2018 audit awareness training discusses what the Board should know about internal controls and risk management principles as it carries out its oversight responsibilities.

PURPOSE:

To provide new and existing Board Members with training on internal controls and risk management principles with a specific focus on the Board's oversight responsibilities. The training session will fulfill the audit awareness training requirements outlined in Article III of the Bylaws of the Washington Metropolitan Area Transit Authority (WMATA) Board of Directors.

DESCRIPTION:

Key Highlights:

Training is designed to increase awareness of internal controls and risk management practices through a discussion of fundamental concepts and internal controls and risk management principles based on guidance from the Committee of Sponsoring Organizations (COSO's) Internal Control – Integrated Framework and Enterprise Risk Management (ERM) - Integrating with Strategy and Performance, the Framework for ERM. Session will highlight Board's oversight responsibilities as it relates to the specific principles from both frameworks.

Background and History:

Audit Awareness Requirement

Article III Section 1 of the Bylaws of the Washington Metropolitan Area Transit Authority Board of Directors identifies the Executive Committee as the Committee responsible for providing oversight of the quality and integrity of WMATA's internal controls, compliance systems, and auditing and accounting systems. As outlined in Committee responsibilities, the Executive Committee is responsible for conducting annual audit awareness training for all Board Members. Under the direction of the Executive Committee, this training session is designed to meet the audit awareness training requirement for new and existing Board Members.

Discussion:

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.

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 for a particular subsidiary, division, operating unit, or business process.
- It 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.

Board Responsibilities for Internal Controls

- Establish oversight structure aligned with 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.
- Evaluate the integrity and ethical values of senior management.
- Evaluate the potential impact of significant changes, fraud, and management override of Internal Control.

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 of Directors have an oversight role for risk across the organization.

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.

Group Discussion

FUNDING IMPACT:

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

TIMELINE:

Previous Actions	Annual Audit Awareness Training – Fraud Awareness – December 14, 2017

Anticipated actions after presentation	N/A

RECOMMENDATION:

-

Annual Audit Awareness Training

Internal Control and Risk Management Principles

Executive Committee
December 13, 2018

Session Objectives

- Increase awareness of Internal Control and Risk Management Principles
- Discuss Board oversight responsibilities for Risk and Internal Controls
- Fulfill the audit awareness training requirements outlined in Article III of the Bylaws of the Washington Metropolitan Area Transit Authority (WMATA) Board of Directors

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)

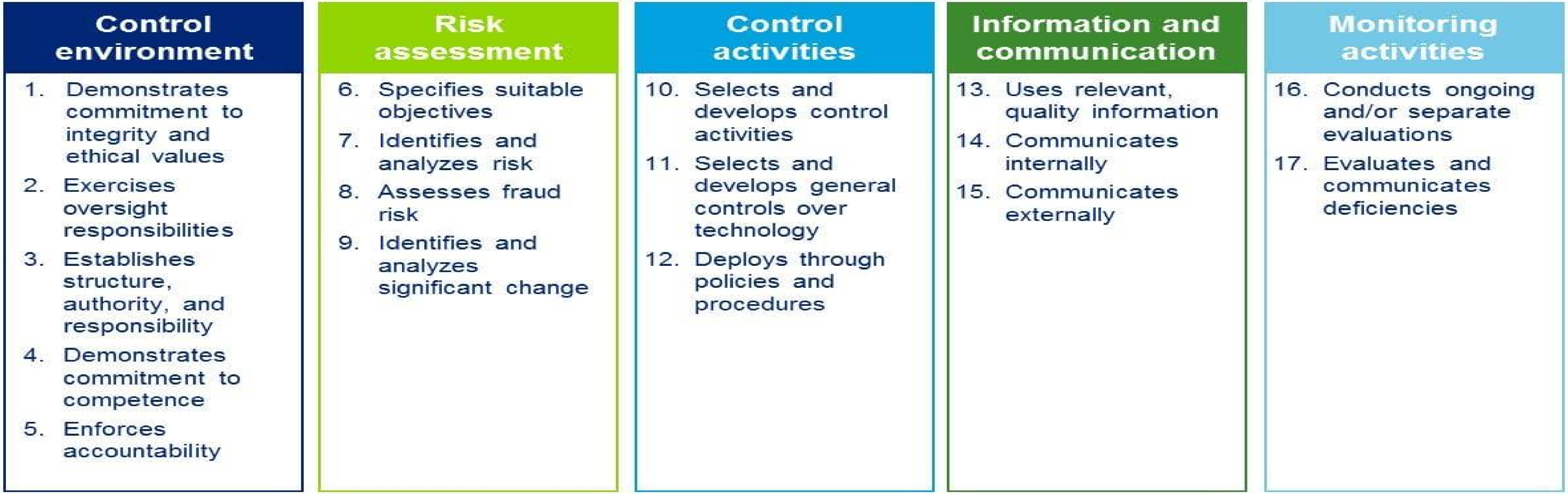
Internal Control — Key Concepts

- Geared to achievement of objectives
- Internal control is a process
- Effected by people
- Provides reasonable assurance
- Adaptable to entity structure and flexible in application
- Involves plans, methods, policies and procedures

Internal Control — Key Concepts

Internal control is everyone’s responsibility

Internal Control Principles



Control environment	Risk assessment	Control activities	Information and communication	Monitoring activities
1. Demonstrates commitment to integrity and ethical values 2. Exercises oversight responsibilities 3. Establishes structure, authority, and responsibility 4. Demonstrates commitment to competence 5. Enforces accountability	6. Specifies suitable objectives 7. Identifies and analyzes risk 8. Assesses fraud risk 9. Identifies and analyzes significant change	10. Selects and develops control activities 11. Selects and develops general controls over technology 12. Deploys through policies and procedures	13. Uses relevant, quality information 14. Communicates internally 15. Communicates externally	16. Conducts ongoing and/or separate evaluations 17. Evaluates and communicates deficiencies

Source: Committee of Sponsoring Organizations of the Treadway Commission (COSO) – Internal Control Integrated Framework

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)

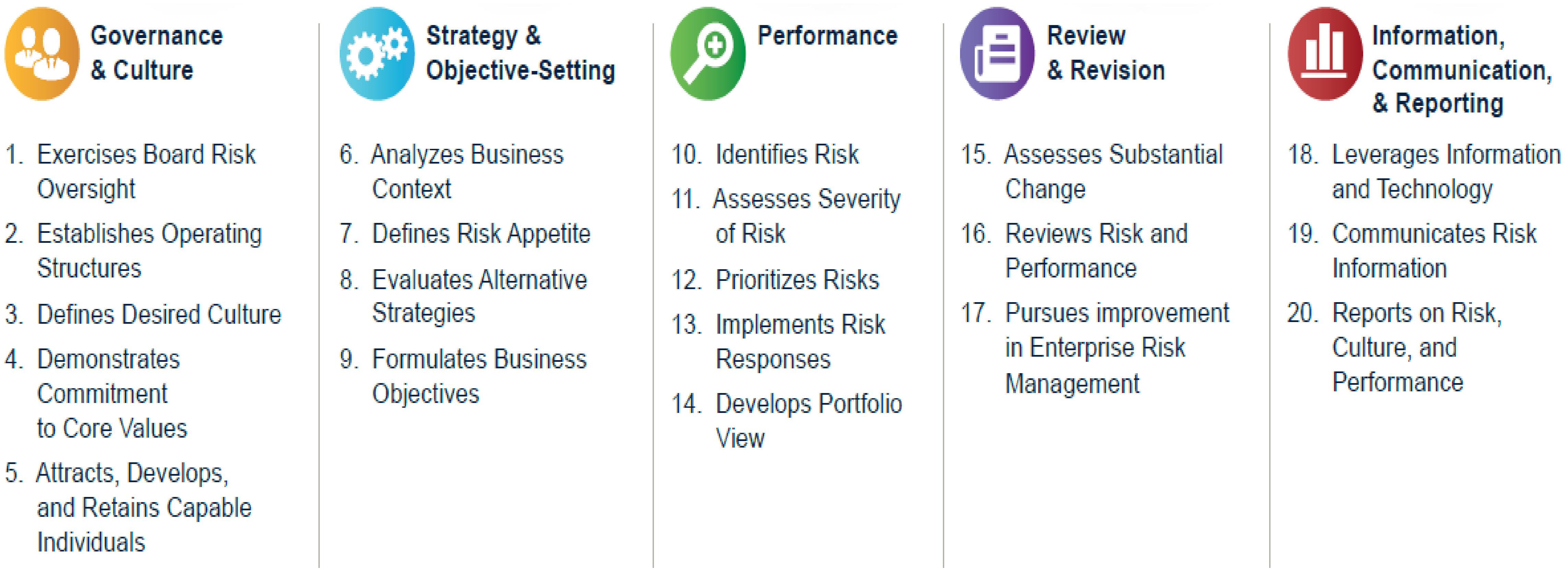
The culture, capabilities, and practices, integrated with strategy-setting and its performance, that organizations rely on to manage risk in creating, preserving, and realizing value. (COSO ERM)

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

Risk Management 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

Governance is Critical

Board of Directors

- Oversight responsibility – govern through policies, set the “tone at the top.”
- 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.

Management

- **GM/CEO** – Responsible for establishing, maintaining and monitoring the system of internal controls and effective risk management practices.
- **Management** – Owns and manage risk and internal controls.
- The Executive Management Team (EMT), Directors and Managers are accountable for the design and operating effectiveness of internal controls and other mitigating actions that respond to risk.

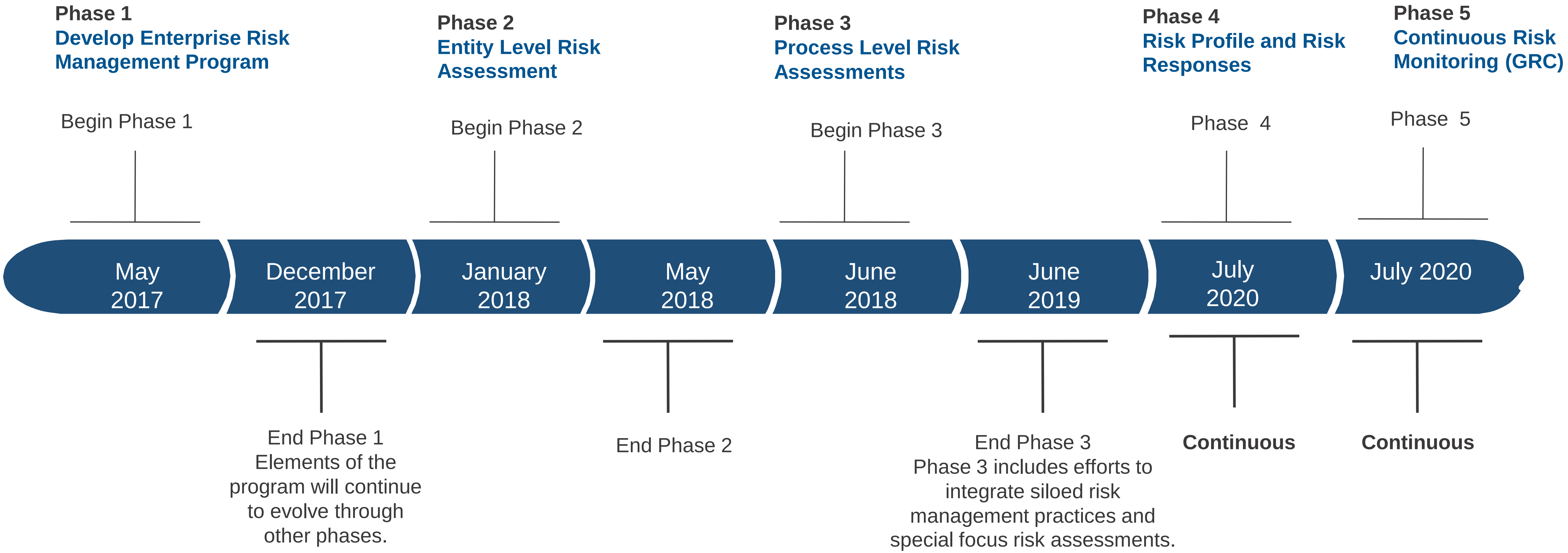
Board Oversight Responsibility — Risk and Internal Controls

Are you asking the right questions about

&

?

ERM Implementation Timeline



Phase 1
Develop Enterprise Risk Management Program

Phase 2
Entity Level Risk Assessment

Phase 3
Process Level Risk Assessments

Phase 4
Risk Profile and Risk Responses

Phase 5
Continuous Risk Monitoring (GRC)

Begin Phase 1

Begin Phase 2

Begin Phase 3

Phase 4

Phase 5

May 2017

December 2017

January 2018

May 2018

June 2018

June 2019

July 2020

July 2020

End Phase 1
Elements of the program will continue to evolve through other phases.

End Phase 2

End Phase 3
Phase 3 includes efforts to integrate siloed risk management practices and special focus risk assessments.

Continuous

Continuous

Risk Categories and Elements

Service Delivery

- Asset Management
- Business Interruption
- Knowledge Management
- Process Efficiency
- Supply Chain
- Training & Development
- Workforce Competencies
- Empowerment
- Labor Management
- Performance Incentives

Reputation

- Brand/Image and Marketing
- Communications (Internal & External)
- Customer/Stakeholder
- Employee Conduct
- Public Relations

Financial Management

- Financial Management Controls
- Budgeting
- Cash Flow (AP & AR)
- Grants Management

Safety

- Employee & Customer Safety
- General Public Safety
- Natural Disaster
- Physical Security

Legal and Compliance

- Legal, Illegal & Fraud Acts
- Policies & Procedures
- Political & Regulatory Changes
- Third Party (Counterparty)

Strategic

- Capacity
- Innovations
- New Projects & Programs
- New Initiatives

Information Technology

- Cyber Security
- Access
- Completeness & Accuracy
- Data Integrity
- Information Availability
- Information Management
- Integrated Systems
- IT System Reliability
- Technological Innovation
- Logical Security

Top Ten Risks

Infrastructure Disrepair

Cybersecurity and Inappropriate Access

Litigation and Fraud

Workforce Planning and Talent Management

Asset Management Information

Policies, Procedures and Compliance

Reputation and Stakeholder Perception

Culture

IT Infrastructure Reliability and Technology Advances

Management and Labor Union Relationships

Top Ten Risks for calendar Year 2018 as assessed by Executive Management.

🟦 Top risk noted by other transit agencies and other organizations

Session Summary

- Risk and internal controls are important to the success of any organization.
- Board has oversight responsibilities for risk and internal controls.
- Management is the first line of defense for risk and internal controls.
- Communication is key to an effective risk management process.
- Risk awareness not only includes known significant risks, but also considers emerging risks.