METROPOLITAN TRANSPORTATION AUTHORITY
ENTERPRISE RISK MANAGEMENT AND
INTERNAL CONTROL GUIDELINES

Pursuant to Public Authorities Law Section 2931

Updated and Adopted by the Board on March 25, 2020

These guidelines apply to the Metropolitan Transportation Authority ("MTA") , the New York City Transit Authority, the Long Island Rail Road Company, The Metro-North Commuter Railroad Company, Staten Island Rapid Transit Operating Authority, Manhattan and Bronx Surface Transit Operating Authority, MTA Construction & Development, MTA Bus Company, Triborough Bridge and Tunnel Authority, and to all future affiliated or subsidiary agencies of the MTA (each of which is referred to severally and together, as the "Authority").

Article I. Purpose of Guidelines

The purpose of these guidelines is to establish an effective system of internal controls for the Authority which complies with the requirements of the New York State Government Accountability, Audit and Internal Control Act of 1999 ("the Act") amending Public Authorities Law ("PAL") Sections 2930 through 2932, and is consistent with the Standards for Internal Control in New York State published by the Office of the State Comptroller ("Comptroller Standards"), Guidelines issued by the Independent Authority Budget Office ("IABO"), standards established by the U.S. Government Accountability Office (GAO), and the Commission of Sponsoring Organizations of the Treadway Commission ("COSO") standards.

Article II. Requirements of the Act

In compliance with the requirements of PAL Section 2931 the MTA Board is required to:

1. Establish and maintain for the Authority guidelines for a system of internal control that are in accordance with the Act and internal control standards;

2. Establish and maintain for the MTA a system of internal controls and a program of internal control review. The program of internal review shall be designated to identify internal control weaknesses, identify actions that are needed to correct these weaknesses, monitor the implementation of the necessary corrective actions and periodically assess the adequacy of the Authority's ongoing internal controls;

3. Make available to each member, officer and employee a clear and concise statement of the generally applicable managerial policies and standards with which he or she is expected to comply. Such statement shall emphasize the importance of effective internal controls to the Authority and the responsibility of each member, officer and employee for effective internal control;

4. Designate an internal control officer who shall report to the head of the Authority to implement and review the internal control responsibilities established pursuant to this section; and

5. Implement education and training efforts to ensure that Board Members, officers and employees have achieved adequate awareness and understanding of internal control standards and, as appropriate, evaluation techniques.

Article III. Guidelines Maintenance

These guidelines are subject to annual review by the Audit Committee. In advance of submission of these guidelines for such review, the Enterprise Risk Management Committee ("the Committee" defined in Article IV(B)) shall be responsible for preparing any proposed revisions to the guidelines necessary to ensure that they continue to be in compliance with the Act and consistent with the Comptroller standards, IABO guidelines and COSO standards.

Article IV. Enterprise Risk Management and Internal Controls

Section A. Internal Controls

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.

The definition emphasizes that internal control is:

- Geared to the achievement of objectives in one or more separate but overlapping categories – operations, reporting, and compliance
- A process consisting of ongoing tasks and activities - it is a means to an end, not an end in itself
- Effected by people – it is not merely about policy and procedure manuals, systems, and forms, but about people and the actions they take at every level of an organization to effect internal control
- Able to provide only 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

The Framework provides for three objectives, which allow Authority to focus on separate aspects of internal control:

Operations Objectives - These pertain to effectiveness and efficiency of the entity's operations, including operational and financial performance goals, and safeguarding assets against loss.

Reporting Objectives - These pertain to internal and external financial and non-financial reporting and may encompass reliability, timeliness, transparency, or other terms as set forth by regulators, standard setters, or the Authority's policies.

Compliance Objectives - These pertain to adherence to laws and regulations to which the entity is subject.

A direct relationship exists between objectives, which are what an entity strives to achieve, components, which represent what is required to achieve the objectives, and Authority structure (the operating unit, legal entities, and other structure). Internal control consists of five interrelated components and seventeen principles. All components and principles are relevant in establishing an effective internal control system for the Authority. In order for the authority to have an effective internal control system, the components of internal control must be successfully designed, implemented, and functioning sufficiently. The principles represent the fundamental concepts which are associated with particular components within the system and apply to strategic, operating, reporting and compliance objectives. Below is a summary of each of the five components of internal control.

1. **Control Environment** – The control environment is the set of standards, processes, and structures that provide the basis for carrying out internal control across the organization. The board of directors and senior management establish the tone at the top regarding the importance of internal control including expected standards of conduct. Management reinforces expectations at the various levels of the organization. The control environment comprises the integrity and ethical values of the organization; the parameters enabling the board of directors to carry out its governance oversight responsibilities; the organizational structure and assignment of authority and responsibility; the process for attracting, developing, and retaining competent individuals; and the rigor around performance measures, incentives, and rewards to drive accountability for performance. The resulting control environment has a pervasive impact on the overall system of internal control.

2. **Risk Assessment** – Every entity faces a variety of risks from external and internal sources. Risk is defined as the possibility that an event will occur and adversely affect the achievement of objectives. Risk assessment involves a dynamic and iterative process for identifying and assessing risks to the achievement of objectives. Risks to the achievement of these objectives from across the entity are considered relative to established risk tolerances. Thus, risk assessment forms the basis for determining how risks will be managed.

   A precondition to risk assessment is the establishment of objectives, linked at different levels of the entity. Management specifies objectives within

categories relating to operations, reporting, and compliance with sufficient clarity to be able to identify and analyze risks to those objectives. Management also considers the suitability of the objectives for the entity. Risk assessment also requires management to consider the impact of possible changes in the external environment and within its own business model that may render internal control ineffective.

3. **Control Activities** – Control activities are the actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out. Control activities are performed at all levels of the entity, at various stages within business processes, and over the technology environment. They may be preventive or detective in nature and may encompass a range of manual and automated activities such as authorizations and approvals, verifications, reconciliations, and business performance reviews. Segregation of duties is typically built into the selection and development of control activities. Where segregation of duties is not practical, management selects and develops alternative control activities.

4. **Information and Communication** – Information is necessary for the entity to carry out internal control responsibilities to support the achievement of its objectives. Management obtains, generates and uses relevant and quality information from both internal and external sources to support the functioning of other components of internal control. Communication is the continual, iterative process of providing, sharing, and obtaining necessary information. Internal communication is the means by which information is disseminated throughout the organization, flowing up, down, and across the entity. It enables personnel to receive a clear message from senior management that control responsibilities must be taken seriously. External communication is twofold: it enables inbound communication of relevant external information, and it provides information to external parties in response to requirements and expectations.

5. **Monitoring** – Ongoing evaluations, separate evaluations, or some combination of the two are used to ascertain whether each of the five components of internal control, including controls to affect the principles within each component, is present and functioning.

   Ongoing evaluations, built into business processes at different levels of the entity, provide timely information. Separate evaluations, conducted periodically, will vary in scope and frequency depending on assessment of risks, effectiveness of ongoing evaluations, and other management considerations. Findings are evaluated against criteria established by regulators, recognized standard-setting bodies or management and the board of directors, and deficiencies are communicated to management and the board of directors as appropriate.

The principles supporting the components of internal controls are listed below:

Control Environment

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

Risk Assessment

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

Control Activities

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

Information and Communication

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

Monitoring

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

In the event that management determines that a principle is not relevant, such determination should be at a minimum be supported with documentation and a rational of how, in the absence of that principle, the control is operating effectively.

Supporting each principle are points of focus, representing important characteristics associated with the principles. Point of focus are intended to provide helpful guidance to assist management in designing, implementing and conducting internal control and in assessing whether relevant principles are present and functioning.

Section B. Enterprise Risk Management

Enterprise risk management addresses more than internal controls. It also addresses other topics such as strategy-setting, governance, communicating with stakeholders and measuring performance. Its principles apply at all levels of the organization and across all functions.

Enterprise Risk Management ("ERM") is defined as the culture, capabilities, and practices, integrated with strategy-setting and performance, that organizations rely on to manage risk in creating, preserving, and realizing value.

Enterprise risk management consists of five components and twenty principles. These components are:

1. **Governance & Culture** – Governance sets the Authority's tone, reinforcing the importance of, and establishing oversight responsibilities for, enterprise risk management. Culture pertains to ethical values, desired behaviors, and understanding of risk in the entity.

2. **Strategy and Objective-Setting -** Enterprise risk management, strategy, and objective-setting work together in the strategic-planning process. A risk appetite is established and aligned with strategy; business objectives put strategy into practice while serving as a basis for identifying, assessing, and responding to risk.

3. **Performance** - Risks that may impact the achievement of strategy and business objectives need to be identified and assessed. Risks are prioritized by severity in the context of risk appetite. The organization then selects risk responses and takes a portfolio view of the amount of risk it has assumed. The results of this process are reported to key risk stakeholders.

4. **Review and Revision** - By reviewing entity performance, an organization can consider how well the enterprise risk management components are functioning over time and in light of substantial changes, and what revisions are needed.

5. **Information, Communication, and Reporting** - Enterprise risk management requires a continual process of obtaining and sharing necessary information, from both internal and external sources, which flows up, down, and across the organization.

Enterprise Risk Management Principles

The five components are supported by a set of principles. These principles cover everything from governance to monitoring. These principles are:

Governance & Culture

1. Exercises board risk oversight
2. Establishes operating structures
3. Defines desired culture
4. Demonstrates commitment to core value
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

Section C. Enterprise Risk Management Committee

The Enterprise Risk Management Committee ("the Committee") has the authority and responsibility for ensuring compliance by the Authority with the Act, Comptroller Standards, IABO guidelines and COSO standards. In addition, the Committee has authority to oversee the ERM program as it relates to all MTA Business occur between multiple Agencies and may also:

- Advise on risk strategy,
- Assist with identifying risk appetite and tolerance
- Oversee risk exposures
- Review crisis management plans, and
- Support the internal control program

Each Agency Risk Officer and other relevant MTA Staff may serve on the Committee, which is chaired by the MTA Chief Ethics, Risk and Compliance Officer. The Committee will meet as needed but generally not less than every quarter to review and suggest improvements to the ERM program.

Section D. Vulnerability Assessments

Part 1. Components

Vulnerability (Risk) Assessments ("VA") is an analysis of potential threats to critical business functions. The VA identifies existing controls and controls need to be added or modified to manage risk. The VA also defines how often and when controls are to be tested. Each VA must at a minimum contain the following:

- Identification of key business processes
- Objectives of each business process
- Risks to those objectives
- Effect and likelihood (in the absence of controls) of risks occurring and an overall vulnerability rating
- Controls in place to manage each risk to an acceptable level
- Testing frequency (based on vulnerability rating)
- Testing schedule (approximately when each control will be tested during a particular cycle)

Part 2. Controls

Controls will be classified as key, subordinate, secondary, or monitoring.

Key Controls – an internal control that is assessed by management that provides reasonable assurance that material errors will be prevented or detected in a timely manner and that without which the business process will break down.

Subordinate Controls – those internal controls that are utilized to supplement key controls. Subordinate controls can be compensating, mitigating or redundant as it relates to the key control.

Secondary Controls – those controls which are not key or subordinate controls.

Monitoring Controls - those controls that are not designed to mitigate risk but are designed to monitor non-critical business process risks.

Part 3. Assessing Risk Effect, Probability, and Overall Risk Rating

Risk within a business process is the probability that a hazard will adversely impact the business process, its objective, and/or related activities. Risk within a business process can be assessed by defining what negative event can reasonably occur (risk), evaluating the significance (effects) and estimating the likelihood that the event can happen (probability). When assessing the risk

effect if the risk occurs the following categories should be used in determining level of significance.

Significance Rating	Evaluation Criteria
High (5)	Will cause a failure of the business process to meet its objectives, or cause objective failure in other activities, which will, in turn, cause or expose the Authority to significant financial losses, interruptions in operations, failure to comply with laws and regulations, major waste of resources, failure to achieve stated goals, etc.
Med High (4)	May cause a failure of the business process to meet a significant part of its objectives, or impact the objectives of other activities, which may, in turn, expose the Authority to unacceptable financial losses, reductions to or ineffectiveness of operations, non-compliance with laws and regulations, sizable waste of resources, etc.
Medium (3)	May cause a failure of the business process to meet part of its objectives, which may, in turn, expose the Authority to unacceptable financial losses, inefficient operations, non-compliance with laws and regulations, waste of resources, etc.
Medium Low (2)	May cause the business process, or other activities, not to meet part of its objectives which, may, in turn, expose the Authority to potentially unacceptable financial losses, less effective or efficient operations, some non-compliance with laws and regulations, waste of resources, etc.
Low (1)	Unlikely to cause the activity not to meet part of its objectives. If the activity does not meet part of its objective, this, in turn, may cause or expose the Authority to potentially unacceptable financial losses, less efficient operations, some non-compliance with laws and regulations, less efficient use of resources, etc.

When assessing the likelihood, the risk will occur the following categories should be used in determining level of likelihood.

Likelihood Rating	Evaluation Criteria (Assumes No Controls in Place)
High	Reasonable assumption that this risk will almost certainly occur
Medium High	Reasonable assumption that this risk will likely, but not certainly, occur
Medium	Reasonable assumption that this risk may occur
Medium Low	Reasonable assumption that this risk will likely not occur
Low	Reasonable assumption that this risk will not occur

Use the overall risk rating to identify the relative importance and required testing of each control. For ease of assessing, the impact of each risk multiply the numeric values associated with the significance rating and the likelihood rating to determine a relative overall risk rating to each risk: Effect x Probability = Vulnerability

Overall Risk Rating				
High	Medium High	Medium	Medium Low	Low

Section E. Control Testing

The frequency of performing an internal control test is determined by the overall risk rating. Risks with very high or high overall risk rating are considered to be more critical than those in lower categories given that controls are used to manage risks to acceptable levels. Therefore, controls over high risk activities must be tested more frequently. The Authority's testing cycle is classified as follows:

Vulnerability	Control Test Cycle
High	Annually (Minimum)
Medium High	Not less than Every 2 years
Medium	Not less than Every 3 years
Medium Low	Not less than Every 4 years
Low	Not less than Every 5 years

Each Business Process Owner along with Risk Manager is responsible for creating test instructions. Test instructions should contain at a minimum the standard which will be used to judge the control, the methods which will be utilized to test the control, the sample size and test period. In addition, the test instructions should include criteria for what constitutes passing versus failing of any given test.

Business Process Owners must maintain records, both electronic and paper, for each test. The records must include when the test was performed, by whom, what was tested, how it was done, scope (period of time covered), number of records reviewed, personnel involved, personnel interviewed, actions observed, errors found, conclusions and corrective action plans to be implemented. Records must be maintained at a minimum through at least one internal control review cycle (1-5 years) or as required by Authority's records retention policy.

The Committee shall establish standards for testing for the ERM business processes.

The Business Process Owners must provide proof of testing, including copies of all testing records at the request of the MTA Corporate Compliance, MTA Audit Services, or the MTA Inspector General Office. Failure to provide testing documentation must be reported to the Chief Compliance Officer and the Agency President.

Section F. Internal Control Review and Assessment

The Authority shall conduct an annual Internal Control Review and Assessment ("ICRA") which is an examination and evaluation of the Authority's system of internal controls to ascertain whether adequate controls exist to:

- Encourage adherence to Authority's policies and procedures
- Promote operational efficiency and effectiveness
- Safeguard assets
- Create and maintain a safe environment for employees and customers
- Ensure reliability of accounting data

The results of the ICRA, at a minimum, reaffirms that there is reasonable assurance that controls are functioning as intended.

Based upon the result of the ICRA, the Authority's shall complete, as part of its Annual Report, an annual assessment of the effectiveness of internal control structures and procedures. The assessment is a written statement from the MTA Chief Compliance Officer setting forth the Authority has conducted a formal, documented process to assess the effectiveness of its internal control structure and procedures, and indicating whether the internal controls are adequate.

Section G. Certification and Summary Reports

The Chairman/Chief Executive Officer on behalf of the Authority shall complete a signed certification and summary report that the Authority's internal control program is compliant with the Act. In support of this certification, each Agency President shall also sign a certification and summary report that their Agency is compliant with the Act.

Section H. Corrective Action Plans

If any control should fail the Control Testing or ICRA process, described in Section D and E above, a corrective action plan must be initiated. The corrective action plans will at a minimum list the severity of the issue as either:

- Material Weakness
- Significant Deficiency
- Deficiency
- Documentation Only

This corrective action plan shall also include:

- Actions to be undertaken
- Persons responsible for those actions
- Resources required to complete the corrective action
- Date corrective actions were completed or date by which they are expected to be achieved

Article V. Generally Applicable Managerial Policies and Standards

The Chairman/Chief Executive Officer of the Authority, together with Agency Presidents shall prepare and disseminate annually a statement emphasizing the tone at the top, the importance of effective internal controls and the responsibility of each officer and employee for effective internal controls. This statement should list the name and contact number of the Risk Officer assigned to their respective Agency and any other individuals who can be contacted for further information on internal controls.

Managerial policies and procedures for the performance of specific functions shall be articulated in administrative manuals, employee handbooks, job descriptions and applicable policy and procedure manuals. While it is not necessary for all employees to possess all manuals, employees should be provided with, or have access to, applicable policies and procedures for their position.

Each Agency shall establish procedures for policy lifecycle management, including but not limited to the creation, approval, maintenance, storage, monitoring and review of Agency specific policies and procedures. MTA Corporate Compliance shall establish procedures for all agency policy lifecycle management, including but not limited to the creation,

approval, maintenance, storage, monitoring and review of All Agency Policy Directives and Guidelines.

Article VI. Designation of an Internal Control Officer

The MTA Chief Compliance Officer shall serve as Internal Control Officer for the Authority and shall report to the Chairman and Chief Executive Officer of the Authority or his/her designee. The Chief Compliance Officer shall implement and review the internal control responsibilities established by these guidelines to ensure compliance by the Authority.

Article VII. Implementation of Education and Training Programs

Senior management and employees responsible for specific functions relating to the Authority's internal control program must attend recurring internal control training.

The training will utilize standardized material on Internal Controls developed by the Committee as well as the Office of the New York State Comptroller's Internal Control Guide-Compliance Road Map. Agencies may augment this guide, if necessary, to provide specialized instruction.

The Committee shall determine at a minimum which classification of employees should attend internal control training, including the method, content and frequency of such training.

Article VIII. MTA Audit Services

In order to maintain independence, MTA's Auditor General and MTA Audit Services shall not directly or indirectly manage the Authority's ERM/Internal Control program. MTA Audit Services shall evaluate the Authority's internal controls and operations, identify internal control weaknesses that have not been corrected and make recommendations to correct those weaknesses.