METROPOLITAN TRANSPORTATION AUTHORITY
ENTERPRISE RISK MANAGEMENT AND
INTERNAL CONTROL GUIDELINES

Pursuant to Public Authorities Law Section 2931

Adopted by the Board on November 16, 2016

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 Capital Construction, 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 replace MTA All Agency Policy Directive 11-008 Accountability & Internal Control issued June 8, 1990.

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. System of Internal Controls and Program of Internal Control Review

Section A. Enterprise Risk Management/Internal Controls

Enterprise Risk Management ("ERM")/Internal Controls is defined as a process conducted by the Authority's Board, management and other personnel, applied in a strategic setting and across the Authority, designed to identify potential events that may affect the entity, and manage risk to be within risk appetite, to provide reasonable assurance regarding the achievement of objectives in the following categories:

Strategic - high-level goals, aligned with and supporting Authority's mission
Operations - effective and efficient use of the Authority's resources
Reporting – reliability, timeliness, transparency of financial and non-financial reporting
Compliance - compliance with applicable laws, regulations, contracts and policies

The definition reflects certain fundamental concepts regarding ERM/Internal Control management. ERM/Internal Control management is:

- An ongoing and flowing process throughout the Authority
- Effected by people at every level within the Authority
- Applied in developing and implementing strategy
- Applied across the Authority, at every level and in all areas of responsibility

- Designed to identify potential risks that, if they occur, will affect the Authority

ERM/Internal Controls consists of eight interrelated components. These components are:

1. **Control Environment** – The internal environment encompasses the tone of the Authority, and sets the basis for how risk is viewed and addressed by employees, including risk management philosophy, integrity and ethical values, and the environment in which they operate.

2. Objective Setting – Objectives must exist before management can identify potential events affecting their achievement. Internal control management ensures that management has in place a process to set objectives and that the chosen objectives support and align with the Authority's' mission.

3. Event Identification – Internal and external events affecting achievement of Authority's objectives must be identified, distinguishing between risks and opportunities.

4. **Risk Assessment** – Risks are analyzed by, considering likelihood and impact, as the basis for computing the overall risk rating. The vulnerability of the Authority to various risks determines how they should be managed.

5. Risk Response – Management evaluates the available risk response options (avoiding, accepting, reducing or sharing) and selects the strategy that optimizes the cost-benefit goals of the Authority.

6. **Control Activities** – Policies and procedures are established and implemented to ensure that the risk responses strategy is established and effectively executed.

7. **Information and Communication** – Relevant information is identified, analyzed, and communicated in a form and timeframe that enable employees to effectively carry out their responsibilities.

8. **Monitoring** – Internal Controls are monitored and modifications made as necessary. Monitoring is accomplished through ongoing management activities, separate periodic evaluations, or both.

Internal Control 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. 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.

Section B. 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 those Business Processes and their associated risks and controls that 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

Authority Internal Control Officers or their designees serve on the Committee, which is chaired by the MTA Chief Compliance Officer. The Committee will meet as needed but generally not less than every six months to review and suggest improvements to the ERM program.

Section C. Vulnerability Assessments

Part 1. Components

Vulnerability (Risk) Assessments ("VA") is an analysis of the potential exposure to a thing going wrong, what can happen if it does, and what controls, if any, are or should be in place 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 inherent potential for events to occur that will negatively impact that business process, its objectives, and/or related activities. Vulnerability within a business process can be assessed by defining what negative event can reasonably occur (risk), evaluating their significance (effects) and estimating the likelihood that they can happen (probability). When assessing the 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 occurs the following categories should be used in determining level of likelihood.

Likelihood Rating	Evaluation Criteria (Assumes No Controls in Place)
Extreme (5)	Reasonable assumption that this risk will almost certainly occur
High (4)	Reasonable assumption that this risk will likely, but not certainly, occur
Medium (3)	Reasonable assumption that this risk may occur
Low (2)	Reasonable assumption that this risk will likely not occur
Negligible (1)	Reasonable assumption that this risk will not occur

The overall risk rating is used 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				
Very High (25-20)	High (19-16)	Medium (15-9)	Low (8-4)	Very Low (3-1)

Section D. 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
Very High	Annually (Minimum)
High	Not less than Every 2 years
Moderate	Not less than Every 3 years
Low	Not less than Every 4 years
Very Low	Not less than Every 5 years

Each Business Process Owner along with their Authority Internal Control Officer 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 Chief Compliance Officer, the Authority ICO for their respective Agency, 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 E. 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 or not the internal controls are adequate.

Section F. 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 G. 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 Authority Internal Control Officer for 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.

Each MTA Agency President shall appoint an Authority Internal Control Officer, who shall report to the Agency President or to his/her designee within the executive office

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.