



**THE CITY OF NEW YORK
OFFICE OF THE COMPTROLLER**

INTERNAL CONTROL AND ACCOUNTABILITY DIRECTIVES

DIRECTIVE #1: PRINCIPLES OF INTERNAL CONTROL

INTRODUCTION

Internal Control must form an integral part of an agency's management plans. Effective internal controls are necessary to achieve objectives, assure full accountability for resources, and mitigate a broad range of risks. Effective internal controls over agency financial activities also ensure the reliability of New York City's accounting systems and financial reporting.

Internal Control is defined by the United States Government Accountability Office (GAO) as a process affected by an entity's management which is designed to provide reasonable assurance that agency objectives—including reliable financial reporting, effective and efficient operations, and compliance with applicable laws and regulations—are met.

This Directive outlines the principles of a sound and effective internal control system that should be adopted by the City and its agency management and staff. This Directive is broadly consistent with the internal control framework described by GAO in its *Standards for Internal Control in the Federal Government* (“Greenbook”).

This Directive also amends the original requirement that agencies complete the Directive #1 Financial Integrity Checklist (“Checklist”) with an Agency Financial Integrity Statement (“Statement”) annually, to once every four years.

The Checklist and Statement represent the minimum questions that agency management should ask, and minimum criteria that they should follow, in assessing and designing a reliable and effective system of internal controls. These are not intended to cover every conceivable risk; these are intended to provide a reasonable assurance that major risks that are common across City agencies have been considered and internal controls established in response.

The Office of the Comptroller (“Office”) evaluates responsive documents and may request supporting information and documentation to gain a better understanding of the internal control systems established by agencies. The Office may also audit the information presented by agencies or incorporate an assessment of internal controls during performance audits of agency programs. Generally accepted government auditing standards (adopted in the New York City Charter as the standard for this Office’s audits) require auditors to evaluate internal controls if necessary to achieve audit objectives.

This Directive is issued pursuant to this Office’s authority as provided in Chapter 5, Section 93 of the [New York City Charter](#).

TABLE OF CONTENTS

1. GENERAL INFORMATION.....	4
1.1 <i>Effective Date</i>	4
1.2 <i>Assistance</i>	4
1.3 <i>Comptroller's Internal Control and Accountability Directives</i>	4
2. GENERAL CHARACTERIZATION.....	4
3. FUNDAMENTAL CONCEPTS.....	4
3.1 <i>Continuous and Integral Component of Operations</i>	4
3.2 <i>Requires Management and Staff Involvement</i>	5
3.3 <i>Affords Only Reasonable Assurance</i>	5
4. STANDARDS OF CONTROL.....	6
4.1 <i>Control Environment</i>	6
4.2 <i>Risk Assessment</i>	7
4.3 <i>Control Activities</i>	7
4.4 <i>Information and Communications</i>	8
4.5 <i>Monitoring</i>	8
5. LEVELS OF INTERNAL CONTROL.....	9
5.1 <i>Top Level Agency Performance Reviews</i>	9
5.2 <i>Management Review at Functional or Activity Level</i>	10
5.3 <i>Workforce Management</i>	11
5.4 <i>Control Over Computer Information Processing</i>	11
5.6 <i>Segregation of Duties</i>	12
5.7 <i>Proper Execution of Transactions and Events</i>	12
5.8 <i>Accurate and Timely Recording</i>	12
5.9 <i>Access Restrictions to Records and Resources</i>	12
5.10 <i>Appropriate Documentation of Transactions and Internal Controls</i>	13
6. AGENCY FINANCIAL INTEGRITY STATEMENT AND CHECKLIST	13

1. GENERAL INFORMATION

1.1 *Effective Date*

This Directive is effective immediately.

1.2 *Assistance*

Agencies that have questions, require assistance, or wish to comment on this Directive should email the Audit Bureau at audit@comptroller.nyc.gov.

1.3 *Comptroller's Internal Control and Accountability Directives*

An inventory of existing *Comptroller's Internal Control and Accountability Directives* is available on the [*Comptroller's Website*](#).

2. GENERAL CHARACTERIZATION

Internal controls are a fundamental component of accountability of every agency's operation. Well-designed and adequately monitored internal controls provide safeguards against a broad range of potential risks to an agency.

Internal controls should provide reasonable assurance that the objectives of the agency are being achieved in the following categories:

- Effectiveness and efficiency of operations.
- Appropriate use and safeguarding of all resources and assets.
- Reliability of financial reporting on budget execution and in financial statements.
- Compliance with all applicable laws and regulations.
- Reliability and security of data that is collected and maintained.
- Accuracy of internal and external reporting against established goals and key performance indicators.

3. FUNDAMENTAL CONCEPTS

The following fundamental concepts provide a framework for designing an effective internal control environment.

3.1 *Continuous and Integral Component of Operations*

Internal controls consist of a series of actions or activities that operate as built-in components of an agency's operations. Internal controls must be an integral part of an agency's process and should be supported by a monitoring and reporting structure.

Monitoring is necessary to ensure internal controls established as part of the day-to-day business process have been implemented, are being carried out, and are effectively mitigating risk. Internal controls should be periodically reviewed and assessed for adequacy.

3.2 Requires Management and Staff Involvement

All personnel in an organization participate in ensuring internal controls are effective. Management's responsibility for internal control extends beyond creating the system's structure and mechanisms. Management must also ensure the existence of a healthy internal control environment throughout the agency.

Management's visible support for effective internal control systems is essential. This includes providing the resources necessary to establish and monitor internal control systems; mandating periodic reviews of risk and associated internal controls; ensuring internal controls are established in response to certain triggering events (referred to below under Risk Assessment); supporting measures that increase and enhance individual and agency accountability; conducting internal audits; implementing changes in response to internal and external audit findings; and ensuring agency management does not routinely bypass or deviate from established internal controls.

Staff should understand, accept, and participate in the establishment and implementation of controls. Staff will likely perform many of the tasks that are intended to achieve control as part of day-to-day business operations, so they need to know what is expected of them, and why. Internal controls should be written into policy and procedure documents, and regular training to reinforce such policies and procedures should be provided to staff.

Every City employee also has an affirmative obligation to report, directly and without undue delay, to the Commissioner of Investigation or an Inspector General any and all information concerning conduct which they know or should reasonably know to involve corrupt or other criminal activity or conflicts of interest, (i) by another City officer or employee, which concerns his or her office or employment, or (ii) by persons dealing with the City, which concerns their dealings with the City ([Mayoral Executive Order 16](#)).

3.3 Affords Only Reasonable Assurance

Well-structured internal controls provide only reasonable, not *absolute* assurance, that agency operations are protected from risk. Establishing an effective system of internal controls requires management to identify and rate risks by severity and to focus efforts on mitigating risks that represent the most danger to the agency, within the categories outlined in Section 2. This is done in part by balancing the consequences of failing to prevent or detect specific risks against the cost and feasibility of establishing controls intended to prevent or reduce such risks.

Risks can broadly be categorized based on the nature of potential consequences if internal controls are not effectively established and monitored, and include litigation risk; risk that essential or mandated services will not be provided as intended; risks of fraud, waste, and abuse; risks of security breaches and improper release of protected information; health and safety risks; risks that agency performance goals will not be met; and reputational risks to the agency and program. This is not an exhaustive list; agencies should include risks that are unique to their operations and assess accordingly.

4. STANDARDS OF CONTROL

The following five control components outline the minimum standards of an internal control system and provide the basis for which an agency's internal controls may be evaluated.

4.1 *Control Environment*

A positive control environment is the foundation of all standards of internal control. Agency leadership is charged with supporting and enforcing the internal control system and for ensuring that internal controls are established and implemented across the organization; that managers and staff charged with carrying out related activities have adequate support, skill, resources, and knowledge; and that appropriate enforcement of internal control mechanisms exist. Here are some of the factors, in more detail:

- Maintaining and demonstrating an atmosphere of teamwork, integrity, and ethical values. Agency management must play an active and visible role and must be seen to endorse and support consistent behavioral values, including a commitment to a viable internal control system.
- Support must be given to staff and management in assessing risk and in developing, implementing, performing, and monitoring internal controls. This takes many forms, including the allocation of appropriate resources, ensuring that skill and knowledge levels support the system of internal controls, and providing clear written guidance (including policies and procedures) and related training. Sound personnel policies and practices are also critical factors in maintaining a motivated and healthy control environment.
- An effective internal control environment requires that the agency's organizational structure reflects assigned spans of control-defined areas of responsibility and authority, and that these are formally supported in writing (for example, in tasks and standards and policies and procedures that incorporate internal control activities).
- Enforcement and accountability are also necessary features. Agencies/programs must hold staff and managers accountable for performing internal control activities.

4.2 Risk Assessment

An effective internal control system hinges on the identification of major risks to the agency and to its various sub-divisions. Risk assessments result in the identification, analysis and prioritization of all major internal and external risks to an agency. Risk environments continually change, and as a result, risk assessments of agencies and various programs within the agencies should be conducted periodically.

Agencies should establish a periodic cycle for conducting risk assessments—across the organization—and in addition, certain events should trigger an immediate re-evaluation of specific areas. Examples of triggering events include: new agency or programmatic objectives are set; new legal or regulatory mandates are established; new processes, policies and/or procedures are established; the results of internal monitoring and/or external reviews of agency operations identify significant errors, internal control weaknesses, and/or poor performance; emergencies that change the control environment or program goals; the establishment of new areas of operation and responsibility; and major organizational changes.

Management should comprehensively identify all potential risks to meeting their objectives (refer to Section 2). Risk identification methods may include qualitative and quantitative ranking activities, management conferences, forecasting and strategic planning, and consideration of findings from audits and other assessments. The specific risk analysis methodology used may vary by agency and program area because of the differences in objectives/goals and the difficulty in quantifying risk levels.

Once risks have been identified, they should be analyzed for significance based on likelihood of occurrence and consequences to the agency/program, those served by the agency, and the City, if identified risks are not effectively mitigated. In other words, risks are ranked based on what would happen if such risks are not effectively mitigated by internal controls.

This process involves making value judgments about the nature of risk, potential consequences, and the agency's risk tolerance.

4.3 Control Activities

Internal control activities help ensure that management's directives are carried out. They consist of the policies, procedures, techniques, and mechanisms used to enforce management's directions, and to ensure that associated risks are reduced to an acceptable level.

Control activities should exist at all levels and functions of an agency. They include a wide range of diverse activities such as approvals, authorizations, verifications, record reconciliations, process monitoring, transaction analyses, performance reviews, security evaluations, and the creation and maintenance of related records that provide evidence of the execution of these activities.

The goal of control activities is to reduce risks to an acceptable level. These should be established and written into policy and procedure documents that specify, among other

things, what activities will be performed; who is responsible for performing them and who is responsible for making sure they were performed; what documentation (including system entries) will be created to show they were performed and reviewed; and how they will be tested periodically to ensure activities were performed, reviewed, and documentation is in order.

4.4 Information and Communications

For an agency to successfully manage and control its operations, it must have a reliable and timely communications system that flows both vertically and horizontally throughout the organization. It must be structured to provide pertinent information relating to internal as well as external events that can affect overall performance.

Management requires both operational and financial data to determine whether they are meeting their agencies' strategic and annual performance goals as well as achieving their goals for the effective and efficient use of resources.

Pertinent operational and financial information must be identified, routinely captured, and distributed in a form and time frame that permits people to perform their duties efficiently. In addition to disciplined internal communication standards, management should ensure that there are adequate means of communicating with, and obtaining information from, external third parties that may have a significant impact on the agency achieving its goals.

In addition, effective information technology management is critical to achieving the useful, reliable, and continuous recording and communication of information. Effective systems can play an integral role in ensuring processes are tracked and performed; to continually assess performance and outcomes; to ensure mandated steps in a workflow have been performed, verified, and authorized; and to capture documentation of these steps. Output from systems in the form of data and reports can also facilitate monitoring and testing of the adequacy of internal controls.

In accordance with Executive Order No. 140, the New York City Office of Technology and Innovation (OTI) is responsible for establishing coordinated citywide policies for information technology, telecommunications, and information security (see [Executive Order No. 140](#)).

4.5 Monitoring

A sound internal control system must be supported by ongoing monitoring at various organizational levels and built into regular business processes. Monitoring is used to ensure that internal control activities are being performed. It is not sufficient to merely implement internal control activities; effective internal control systems must include checks to make sure these activities are occurring, are documented, and are effectively reducing risk to an acceptable level.

On a day-to-day basis, monitoring often consists of second level (or higher) review and

approval. More complex monitoring should include periodic testing, on a sample basis, to ensure that activities were performed, reviewed, and documented, and that controls are working. Reviewing data and information maintained in systems may be included in this process, along with data reliability testing.

At a higher level, comprehensive reviews and audits are used to assess whether internal control mechanisms are working. These may be conducted by an agency's internal audit department, by quality assurance specialists, and by external auditors, such as those of the New York City Office of the Comptroller, New York State Office of the Comptroller, the auditors appointed to conduct the City Audit and Single Audit, and various federal agencies.

These may also include internal evaluations that focus directly on a particular control's or set of controls' effectiveness within a specific time frame. The scope and frequency of separate evaluations should depend primarily on the assessment of risks and the effectiveness of ongoing monitoring procedures. Regular self-assessment of this type can be invaluable to management.

Deficiencies found during ongoing monitoring, through separate evaluations or more comprehensive audits, should be communicated to the individual responsible for the function and at a minimum to the next level of management. Serious matters should be reported to senior management and the Agency Head.

Recent audits performed by the Office of the Comptroller and other entities are replete with examples of serious internal control lapses that could have been alleviated or avoided by an agency's internal monitoring. Agencies are encouraged to read the Scope and Methodology section of audit reports; this section summarizes the testing used by auditors to identify errors, risks, and weaknesses in the internal control system, and provides good examples of monitoring activities that may be undertaken internally. [Reports - Office of the New York City Comptroller](#)

5. LEVELS OF INTERNAL CONTROL

An agency's internal control system should be flexible and allow tailoring of its controls to suit its special needs and changes in circumstance. The controls used by a given agency may be different from those used by others based on differences in perceived threats, assessed risks, the operational and legal environment, availability of resources, and the degree of system reliability and resource availability.

5.1 Top Level Agency Performance Reviews

Senior management should ensure risk assessments occur on an agency-wide basis, periodically and when triggering events occur. Senior management should be aware of and ideally participate in the ranking of risks and decisions that hinge on value judgments concerning risk tolerance. Senior management should visibly support internal control systems and foster organization-wide accountability.

Performance indicators that accurately measure whether agency goals and mandates are being met should be established, and associated processes for collecting, reviewing, and analyzing needed data and information implemented. These should be used to conduct trend analysis at regular, pre-determined intervals. This is an important element in assessing the effectiveness of internal control systems. Negative trends can identify weaknesses in an operation. Where feasible, this occurs in systems of record, but when not feasible, appropriate manual processes should be established.

Weaknesses and error rates that are identified should be the subject of internal review and revised internal control measures implemented to ensure correction. Situations identified by internal reviews, audits, and other forms of monitoring should similarly be addressed. When such weaknesses indicate high and medium level risks of any kind, corrective action should be prioritized by senior management.

These practices should be mandated by senior management.

5.2 Management Review at Functional or Activity Level

Management at this level is responsible for establishing internal control activities, second and additional levels of review, and periodic monitoring activities to ensure they occur. Best practice includes ensuring that all major processes are supported by written policies and procedures that provide staff with clear instructions about tasks that must be performed; how, when, and by whom these will be reviewed and verified; the nature of documentation that must be maintained to provide proof; and how, when, and by whom these activities will be monitored. Training should be provided to staff, reviewers, and those conducting monitoring activities, to ensure mandated processes and lines of responsibility are clearly understood.

The point of second level reviews is to provide verification of task completion as tasks are performed on a day-to-day basis. Whether additional levels of review are needed is a management decision. Monitoring is established to test, on a periodic and sampled basis, whether instructions are being followed, second and higher levels of review are occurring, decisions that require authorization are appropriately authorized, required documentation is maintained, and that policies and procedures are being adhered to. When weaknesses are identified, processes and internal control activities should be reassessed and amended as needed to provide additional risk mitigation, and policies and procedures should be modified accordingly.

As with senior management, managers at the activities and functional levels should make full use of information and data to assess the effectiveness of internal control systems, and to analyze indicators and trends to support overall performance weaknesses. These may trigger more formal internal evaluations, reviews, and/or audits to diagnose and determine causes of performance weaknesses.

5.3 Workforce Management

Effective management of an organization's workforce is essential to achieving desired results and an important part of internal control. Operational successes hinge on personnel being provided with clear guidance, appropriate training, necessary tools, structure, and clearly defined responsibilities. Management should ensure that skill needs are continuously assessed and take all possible steps to support the organization's ability to hire a workforce that has the skills necessary to achieve organizational goals.

Systems for assessing individual performance against appropriate tasks and standards should be in place, and annual performance evaluations against such tasks and standards should occur and be documented. Individual accountability should be fostered in this way.

5.4 Control Over Computer Information Processing

A variety of control activities are used in information processing to ensure that access to hardware, software, and data is limited to only those that management determines should have access.

Management should assess the totality of information and data it collects and maintains and understand associated legal mandates and risks in the IT security environment across the organization. Rules governing access to confidential and sensitive information should be established in consultation with agency legal departments. Internal control activities to ensure rules are enforced should be designed and implemented, and as with other controls, reviewed, monitored, and periodically tested.

IT system security must likewise be assessed and systems of protections established in compliance with OTI guidance. Monitoring, testing, and periodic reviews to identify vulnerabilities should occur.

5.5 Control Over Vulnerable Assets

Agencies must establish controls to secure and safeguard vulnerable assets. Examples include security for and limited access to assets such as cash, cash equivalents, securities, inventories, computers, and other equipment which may be vulnerable to risk of loss or unauthorized use.

Agencies should progressively eliminate the need for collecting cash and cash equivalents and move entirely to the Automated Clearing House (ACH) and third-party online payment mechanisms (many of which rely on ACH processes).

Periodic counting and comparison to control records for all vulnerable assets is an important element of control of these assets. In the case of physical assets, this means establishing effective inventory controls and monitoring to ensure assets are labeled, tracked, and periodically counted. Lists of valuable assets (including, for example, computers, laptops, small printers) should be updated regularly to ensure accuracy.

5.6 Segregation of Duties

Key duties and responsibilities should be segregated and shared among staff members to reduce the risk of error or fraud. This is particularly important in financial transactions and in processing financial transactions on behalf of the City, and should include separating the responsibilities for authorizing transactions, processing and recording them, reviewing the transactions, and handling any related assets. No one individual should control all key aspects of a transaction or event.

When strict segregation of duties is not possible, for example in very small agencies or teams, alternative mitigation measures may be considered and implemented.

5.7 Proper Execution of Transactions and Events

Transactions and other significant events should be authorized and executed only by people acting within the scope of their authority. This is the principal means of assuring that only valid transactions to exchange, transfer, use, or commit resources are initiated or entered into. Approved authorization levels should be documented, updated as necessary, and clearly communicated to managers and employees.

Individuals who are not employees of the City of New York must not be allowed to authorize transactions or commit City resources without the oversight and authorization of appropriate employees.

5.8 Accurate and Timely Recording

Transactions should be promptly recorded to maintain their relevance and value to management in controlling operations and decision making. This applies to the entire process cycle of a transaction or event, from initiation and authorization through its final classification in the agency's records. Sound control activities help ensure that all transactions are timely and accurately recorded.

Agencies should note that in certain auditing standards and regulatory frameworks, documentation that is not created contemporaneously, which does not contain appropriate signatures or other markers denoting review and/or authorization, and/or which are not readily available, may be considered unreliable. This supports the need to ensure that documentation is created in the normal course of business and maintained in accessible formats.

Agencies are also reminded that citywide record retention requirements are established by the Department of Records and Information Services ([DORIS](#)) and must be adhered to.

5.9 Access Restrictions to Records and Resources

Access to agency resources and vital records should be subject to appropriate limitations, and accountability for their custody and use should be clearly assigned and maintained.

Access to confidential information stored in documents must be the subject of appropriate internal controls, to prevent unintended release and exposure. Agencies

should ensure that locations and spaces which house confidential documentation and information have secure entries and lockable storage. Staff should be reminded to safeguard this information and protect documentation containing highly confidential information from view, in the office and working from home. Physical documentation containing highly confidential information should not leave agency premises.

Periodic comparison of the resources with documented review and monitoring should be made to reduce the risk of errors, fraud, and/or misuse or unauthorized alteration.

5.10 Appropriate Documentation of Transactions and Internal Controls

All transactions and significant events need to be clearly documented and the documentation readily available for use or examination. Internal controls should be documented in management administrative policies or operating manuals. All documentation should be properly managed and maintained in accordance with citywide records retention requirements.

6. AGENCY FINANCIAL INTEGRITY STATEMENT AND CHECKLIST

As noted above, the Comptroller's Memorandum entitled Filing of Comptroller's Directive #1 Financial Integrity Statement and its accompanying annual Financial Integrity Statement Checklist, are due every four years.

The Agency Head (e.g., Commissioner, First Deputy Commissioner, Executive Director, etc.) is required to sign the Financial Integrity Statement, which represents a formal opinion regarding the adequacy of the agency's internal control structure. This opinion is supported by the Directive #1 Checklist that agency personnel are required to complete. The Checklist represents the minimum internal control criteria that agency management should consider in developing and maintaining a reliable and effective control system.

The completed Checklist and Statement may inform decisions on what aspects of agency operations should be audited, and where audit objectives require it, they may also be considered when assessing the adequacy of agency internal control systems. This Office may also audit the accuracy of Financial Integrity Statement and Checklist responses as part of the Comptroller's audit responsibilities under Chapter 5, Section 93 of the New York City Charter.

The completed and signed Financial Integrity Statement should be addressed to the sitting Deputy Comptroller for Audit, and emailed to the Comptroller's Office at Directive1@comptroller.nyc.gov, and the Mayor's Office of Operations at Directive1@cityhall.nyc.gov. The email subject should include the agency's name and the Statement should be converted to a PDF file. Email transmissions should include both the PDF file of the Financial Integrity Statement and the Excel Checklist. Please be advised that email transmissions must be no larger than 10 MBs.

[Back to the Beginning of the Directive](#)