The City University of New York

MANAGER'S GUIDE

TO INTERNAL

CONTROLS

All University employees play an important part in maintaining strong internal controls

Office of Internal Audit and Management Services
University Internal Control Office

Table of Contents

INTRODUCTION

As The City University of New York's administrators strive to achieve the University's mission and goals and provide accountability for operations, there is a need to continually assess and evaluate our internal control structure to assure that it is well designed and operating effectively, appropriately updated to meet changing conditions, and provides reasonable assurance that the objectives are being achieved. Specifically, managers need to examine internal controls to determine how well the controls are performing, how they may be improved, and the degree to which they can help identify and address major risks for fraud, waste, abuse, and mismanagement.

This 2016 Manager's Guide to Internal Controls was developed to help you establish and maintain effective internal controls in your departments and should be used in conjunction with the official policies and procedures of the University. Compliance with this guide is expected and is subject to review during internal audits of your department or division. It should be also be understood that this guide is intended to *supplement* New York State Office of the State Comptroller's "Standards for Internal Controls" which managers may use to assess the effectiveness of internal controls and identify important aspects of control that are in need of improvement. Users of this guide (and managers and staff in general) should become familiar with the Standards. In addition, it would be helpful if those who are not experienced in internal control matters have access to persons who have such experience and can provide assistance.

References & Acknowledgements

The City University of New York Office of Internal Control would like to credit the Committee of Sponsoring Organizations of the Treadway Commission (COSO) and various State governments and institutions of higher learning for portions of the material contained in this document.

What is Internal Control?

Internal controls is the process employed to help ensure that the University's business is carried out in accordance with the New York State Office of the State Comptroller's *Standards*, University policies and procedures, applicable laws and regulations, and sound business practices. Internal Controls help to promote efficient operations, accurate financial reporting, protection of assets, and responsible fiscal management. All members of the University community are responsible for internal controls. Each business unit or department head is specifically responsible for ensuring that internal controls are established, properly documented, and maintained for activities within their authority.

The University's internal control methodology has been developed using the COSO (Committee of Sponsoring Organizations of the Treadway Commission) conceptual framework adopted in the *Standards for Internal Controls in New York State Government*. In May 2013, COSO released an update to its Internal Control – Integrated Framework. The 2013 Framework retains the definition of internal control and the COSO cube, including the five components of internal control: Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring Activities.

This guide will provide an overview of the COSO model, including a b r i e f description of the requisite objectives, components, principles, and requirements of an effective system of internal control. Finally, it offers considerations on how various parties within the University may use the Framework by summarizing fundamental internal control practices for various types of transactions and situations. The examples provided are not all-inclusive of every control appropriate for each process or department but, instead, serve as an illustration of the most routine transactions/processes.

COSO's Internal Control—Integrated Framework

COSO's Internal Control – Integrated Framework enables organizations to effectively and efficiently develop systems of internal control that adapt to changing business and operating environments, mitigate risks to acceptable levels, and support sound decision making and governance of the organization.

For management and boards of directors, the Framework provides:

- A means to apply internal control to any type of entity, regardless of industry or legal structure, at the levels of entity, operating unit, or function.
- A principles-based approach that provides flexibility and allows for judgment in designing, implementing, and conducting internal controls—principles that can be applied at the entity, operating, and functional levels.
- Requirements or an effective system of internal control by considering how components and principles are present and functioning and how components operate together.
- A means to identify and analyze risk, and to develop and manage appropriate responses to risks within acceptable levels and with a greater focus on anti-fraud measures.
- An opportunity to expand the application of internal control beyond financial reporting to other forms of reporting, operations, and compliance objectives.
- An opportunity to eliminate ineffective, redundant, or inefficient controls that provide minimal value in reducing risks to the achievement of the entity's objectives.

For external stakeholders of an entity and others that interact with the entity, application of the COSO Framework provides:

- Greater confidence regarding the achievement of entity objectives.
- Greater confidence in the organization's ability to identify, analyze, and respond to risk and changes in the business and operating environments.
- Greater understanding of the requirement of an effective system of internal control.
- Greater understanding that through the use of judgment, management may be able to eliminate ineffective, redundant, or inefficient controls.

Structure of Effective Internal Control Systems

The COSO Framework states that:

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 in the following categories:

- o Effectiveness and efficiency of operations,
- o Reliability of financial reporting, and
- o Compliance with applicable laws and regulations.

Organizations achieve these objectives through the operation of the five interrelated components of internal control. These components provide a framework for understanding internal control and assessing its effectiveness. The concepts embodied in the COSO Framework are frequently presented in terms of a three-dimensional cube that depicts the five components operating *across* each internal **control objective** and *within* all organizational units and activities. Not only does the cube demonstrate the connections between objectives and components, it also illustrates that the control components operate at different levels across the organization – a concept that is often overlooked.

The three categories of objectives—operations, reporting, and compliance—are represented by the columns. The five components are represented by the rows. An entity's organizational structure is represented by the third dimension.

©2013, Committee of Sponsoring Organizations of the Treadway Commission (COSO).

Internal control consists of the following five interrelated components:

Control environment factors include the integrity, ethical values and competence of the entity's employees; management's philosophy and operating style; the way management assigns authority and responsibility and organizes and develops its people; and the attention and direction provided by the Board of Trustees.

Risk assessment is the identification and analysis of risks that have the ability to impede the achievement of stated goals and objectives. It is a precursor for determining how risks should be managed. Preconditions to a risk assessment is the establishment of goals and objectives.

Control activities are the policies and procedures that help ensure management directives are carried out. They help ensure that necessary actions are taken to address risks to achievement of the entity's objectives. They include a range of activities such as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets, and segregation of duties.

Information and communication involves the identification, capture and communication of pertinent information in a form and time frame that enables employees to carry out their responsibilities. Information systems produce reports containing operational, financial, and compliance-related information that make it possible to run and control the business unit.

They deal not only with internally-generated data, but also with information about external events, activities, and conditions necessary for informed business decision-making and external reporting.

Monitoring of internal control activities is accomplished through ongoing controls testing and risk assessment or separate evaluations. It includes regular management and supervisory checks and reviews, and other actions personnel take when performing their duties.

When looking at any one category (Operations, Financial Reporting, Compliance), all five of the components, listed above, must be present and functioning effectively to conclude that internal control over operations is effective.

17 Principles of Internal Control

The most significant change made with the 2013 Framework is the codification of the 17 principles that support the five components of internal control. For effective internal controls, the 2013 Framework requires that (1) each of the five components and the 17 relevant principles be *present* and *functioning*; and (2) the five components must operate together in an integrated manner. *Present* means that the components and relevant principles exist in the design and implementation of the system of internal control, and *functioning* means that the components and relevant principles continue to exist in the operation of the system of internal control.

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. Identifies and analyzes significant change
Control Activities	10. Selects and develops control activities 11. Selects and develops general controls over technology 12. Deploys through policies and procedures
Information & Communication	13. Uses relevant information 14. Communicates internally 15. Communicates externally
Monitoring Activities	16. Conducts ongoing and/or separate evaluations 17. Evaluates and communicates deficiencies

©2013, Committee of Sponsoring Organizations of the Treadway Commission (COSO)

The 2013 Framework also provides example characteristics for each of the 17 principles, called Points of Focus, to assist management in determining whether a principle is present and functioning. These are further summarized in the *Standards for Internal Controls in New York State Government*.

Defining Internal Control at CUNY

The university has adopted the internal control methodology as defined by COSO. According to COSO, internal control is defined as follows:

> *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.*

Applied to a college or university, Internal Control is a process affected by a college or university's governing board (Trustees), administration, faculty, and staff designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- **Operational Objectives**: Effectiveness and efficiency of operations and safeguarding of assets.
- **Reporting Objectives**: Reliability, timeliness, and transparency of internal and external financial and non-financial reporting.
- **Compliance Objectives**: Adherence to laws and regulations.

This definition reflects certain fundamental concepts:

- Internal control is a *process*. It is a means to an end, not an end in itself.
- Internal control is *affected by people*. It's not merely policy manuals and forms, but people functioning at every level of the University.
- Internal control is *geared to the achievement of objectives* in several overlapping categories.
- Internal control can be expected to *provide only reasonable, not absolute, assurance*, to an institution's leaders *regarding achievement of operational, financial reporting, and compliance objectives.*

Internal controls for the University are derived from the way a department administrator or manager runs an academic or administrative unit and are integrated with management processes. The department manager has responsibility for ensuring and demonstrating that all five components of internal control (Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring Activities) are present and operating effectively for developing the detailed policies, procedures, and practices to fit their department's operations and mission.

Control Environment

The control environment set by a department administrator establishes the tone of the business unit, influencing the control conscientiousness of its employees. Control environment factors include an administrator's integrity; the ethical values and competence of his/her employees; the way an administrator assigns authority and responsibility, and organizes and develops the unit's employees. An administrator can help promote a good control environment by:

- holding regular team and one-on-one meetings;
- periodically evaluating staff training needs and providing for staff development;
- clearly communicating performance expectations to staff and providing periodic constructive feedback; and
- clearly articulating positions on ethical issues relating to business so that staff receive a clear, unambiguous message to act in an ethical manner.

Risk Assessment

Risk assessment is the identification and analysis of risks relevant to realizing objectives, and it serves as a basis for determining how the risks should be managed. Risk assessment implies an initial determination of operating objectives, then a systematic identification of those things that could prevent each objective from being attained. In other words, it is an analysis of what could go wrong (or what opportunities could be missed). Risks can pertain to internal and external factors, such as:

- <u>Strategic risks</u> - risks that affect the University's ability to achieve its goals
- <u>Financial risks</u> - risks that may result in a loss of the University's assets
- <u>Operational risks</u> - risks that affect the University's ongoing management processes, such as when new administrative systems are installed
- <u>Compliance risks</u> - risks that affect the University's compliance with externally imposed laws and regulations and internal policies and procedures
- <u>Reputational risks</u> - risks that affect how the University is viewed by outsiders (e.g., prospective students, donors, accreditors)

Not all risks are equal. Some are more likely than others to occur, and some will have a greater impact than others if they occur. So once risks are identified, their probability and significance must be assessed. Finally, having identified and assessed risk, management must decide how to deal with it. In some cases, the decision may be to control it; in others, it may be to accept it.
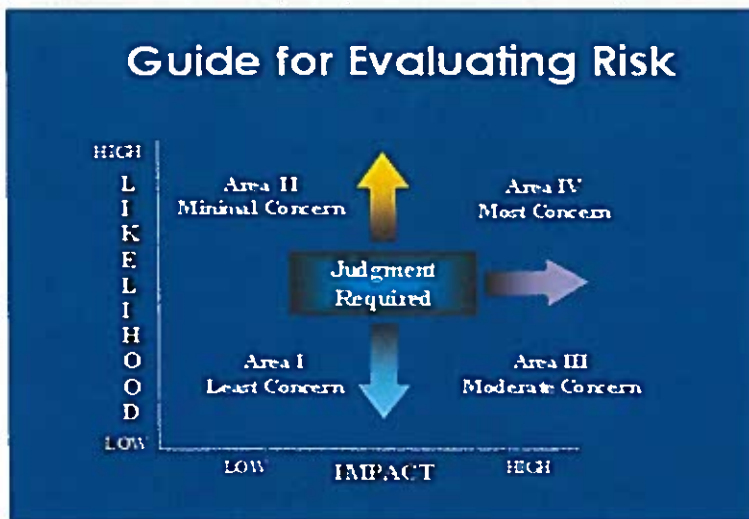
Once risks are identified, management should consider their impact (or significance), the likelihood of their occurrence, and how to manage them.

The process of identifying and analyzing risk is an ongoing process and is a critical component of an effective internal control system.

Control Activities

Control activities are the implementing tools of internal control policy. They 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 include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating procedures, security of assets and segregation of duties. The general guidelines for control activities are outlined below.

- **Segregation of Duties**
  Individual duties are *segregated* so that one person's work routinely serves as a complementary check on another person's work. No one person has complete control over more than one "key" processing function or activity, such as authorizing, approving, certifying, disbursing, receiving or reconciling. For example, individuals responsible for receiving checks in the mail should not be the same individuals that record the receipts.

- **Authorization and Approval**
  Proposed transactions are *authorized* when they are proper and consistent with University policy and organizational plans. Transactions are *approved* by the person delegated approval authority. Approval authority is usually conferred on the basis of some special knowledge or competency. For example, purchase transactions should ultimately be approved by the individual bearing responsibility for the department's budget.

- **Custodial and Security Arrangements**
  The responsibility for the *physical security (custody)* of assets (equipment, inventories, cash and other property) is separated from the related record-keeping (accounting) for those assets. Unauthorized access to assets and accounting systems is prevented.

- **Review and Reconciliation**
  Departmental accounting records and documents 1) are *reviewed* by employees who possess sufficient understanding of the University's financial systems to verify that recorded transactions actually took place and were made in accordance with prescribed procedures; and 2) are *reconciled* with University's financial system reports and financial statements to verify their reasonableness, accuracy and completeness.

Information and Communication

Pertinent information must be identified, captured and communicated in a form and timeframe that enables a manager and staff to carry out their internal control and operational responsibilities efficiently.

Information systems produce reports containing operational, financial and compliance related information that make it possible to run and control a business or academic unit. Effective communication must also occur in a broader sense, flowing down, across and up the unit. All staff must understand their own role in the internal control system, as well as how individual activities relate to the work of others.

Monitoring Activities

Internal control systems need to be monitored -- a process that assesses the quality of the system's performance over time. Ongoing monitoring occurs in the course of normal operations and includes regular management and supervisory activities, such as ongoing supervision, reconciliations, comparisons, performance evaluations, and status reports. In addition, separate operational evaluations are conducted based upon the assessment of risks and the effectiveness of ongoing monitoring procedures. Adequate supervision of personnel and other monitoring activities are required to ensure the reliability of accounting and/or operational controls by pointing out errors, omissions, exceptions and inconsistencies in the application of procedures.

Separate Internal Evaluations

Controls need to be monitored for effectiveness ("Are they are operating as intended?") and to ensure they have not become obsolete. Separate evaluations of control activities can also be useful by focusing directly on the controls' effectiveness at a specific time. The scope and frequency of separate evaluations should depend primarily on the assessment of risks and the effectiveness of ongoing monitoring procedures. Separate evaluations may take the form of self-assessments or the direct testing of internal controls. Deficiencies found during ongoing monitoring or through separate evaluations or testing should be communicated to those responsible for the function and to at least one higher level of management. Serious matters should be reported to top management.

Audit Resolution

Monitoring of internal control should include policies and procedures for ensuring that the findings of audits and other reviews are promptly resolved. Managers are to (1) promptly evaluate findings from audits and other reviews, including those showing deficiencies and recommendations reported by auditors and others who evaluate the department's operations, (2) determine proper actions in response to findings and recommendations from audits and reviews, and (3) complete, within established timeframes, all actions that correct or otherwise resolve the matters brought to management's attention. The resolution process begins when audit or other review results are reported to management, and is completed only after action has been taken that corrects identified deficiencies, produces improvements, or demonstrates the findings and recommendations do not warrant management action.

Who Is Responsible For Internal Control?

Roles and Responsibilities

A system of internal control should be an integral part of the overall responsibility of management to safeguard University, campus and public assets and to continually direct, monitor and improve operations. It should not be a separate and distinct system within the University or college campus, but the embodiment of all the plans and devices which assure reasonable control over operations.

It is the responsibility of management to develop and implement a system of internal controls. However, everyone within the University has some role in internal controls. The roles vary depending upon the level of responsibility and the nature of involvement by the individual. The CUNY Board of Trustees, Chancellor, Presidents and senior administrators establish the presence of integrity, ethics, competence and a positive control environment. The directors and department heads have oversight responsibility for internal controls within their units. Managers and supervisory personnel are responsible for executing control policies and procedures at the detail level within their specific unit.

Internal auditors hold essential responsibilities for assessing, testing, and reporting on internal control. However, internal auditors cannot relieve agency management of its internal control responsibilities. Although internal auditors can provide valuable consultative services with regard to control design, function, and assessment, they cannot relieve management of its responsibility to establish and maintain the internal control system.

The ultimate responsibility for good internal controls rests with the University's and college's own internal management and not with any external unit. The same managers who are responsible for day-to-day operations and decision making are also responsible for ensuring the presence and effectiveness of internal controls within their area of responsibility.

The actual assignment of duties will vary significantly amongst the University's functional units depending on such factors as size and organizational structure. However, it is recommended that consideration be given to the following assignments:

College Internal Control Officer

One *senior* official, having a broad knowledge of the campus operations, personnel and policy objectives, should be designated by the College President as the college internal control officer. This individual should be responsible for coordinating the campus-wide internal control effort and providing visible administrative leadership. This designee should have *sufficient authority* to act on behalf of the campus president to ensure the successful implementation and review of the campus internal control program. Typical duties of this individual as they relate to the internal control effort may include:

- o Preparing, issuing and maintaining campus guidelines
- o Developing campus-specific objectives

- o Chairing a campus steering committee comprised of representatives from key functional areas, i.e., academic, finance and business, and student services
- o Evaluating plans for risk assessments and internal control reviews
- o Coordinating development and presentation of campus-specific training programs for involved staff
- o Monitoring progress
- o Reviewing results of risk assessments and internal control reviews
- o Monitoring the implementation and effectiveness of corrective actions
- o Reporting progress and status to senior campus management

Heads of Major Campus Functional Units

The head, typically the vice president, dean or director, as appropriate, of each major campus functional unit (or other component as identified in the segmenting process) should be responsible for internal control within that unit. Typical duties may include:

- o Participating on a campus steering committee
- o Ensuring that department managers are motivated and trained to accomplish their assignments.
- o Arranging and/or conducting risk assessments and internal control reviews
- o Reviewing and analyzing the results of risk assessments and internal control reviews
- o Ensuring that significant weaknesses in controls are corrected
- o Ensuring that all additions and changes to policies, procedures, systems, etc., include proper controls

Unit Managers

Personnel who are uniquely familiar with individual operations and who are responsible for the management process must take an active role in reviewing and improving controls. On some campuses, the heads of functional units may also perform the duties of line managers. Internal control roles of unit managers may typically include:

- o Establishing an atmosphere within the work environment which is supportive of internal controls
- o Conducting risk assessments and internal control reviews
- o Initiating improved controls when a need is identified
- o Maintaining documentation of controls, risk assessments, internal control reviews and improvements

Internal Controls are an integral part of any organization's financial and business policies and procedures. Internal controls consists of all the measures taken by the organization for the purpose of: (1) protecting its resources against waste, fraud, abuse and inefficiency; (2) ensuring accuracy and reliability in accounting and operating data; (3) securing compliance with the policies of the organization; and (4) evaluating the level of performance in all organizational units of the organization. Our decentralized environment at the University requires that every employee with fiscal responsibility be fully aware of our internal controls requirements.

What is the NYS Internal Control Act?

The New York State Governmental Accountability, Audit and Internal Control Act of 1987 was enacted to assure greater accountability and integrity in State governmental operations. The Internal Control Act requires that all State agencies, including the City University of New York, institute a formal internal control program. The University and each of its campuses must take the following actions toward implementing the Internal Control Act:

- Establish and maintain guidelines for a system of internal controls.
- Establish and maintain a system of internal controls-and a program of internal control review which is designed to identify internal control weaknesses and identify actions that are needed to correct these weaknesses.
- Make a clear and concise statement of the University's/campus's generally applicable management policies and standards with which each employee will be expected to comply be made available to each employee.
- Designate an internal control officer at both the University and campus levels to implement and review the University's/campus's Internal Control Program.
- Implement education and training efforts to ensure employee awareness and understanding of internal control standards and evaluation techniques.
- Periodically evaluate the need for an internal audit function.

The Internal Control Act directs each state agency head to provide an annual statement as to whether the agency's internal controls comply with the prescribed standards. Essentially, this requires a declaration and certification from the Chancellor to the State that the University as a whole complies with such requirements. In addition, the University is to identify and report material weaknesses and indicate plans and schedules for correcting those weaknesses.

Annual Internal Control Certification and Reporting

NYS Division of Budget's B-350 - Governmental Internal Control and Internal Audit Requirements

On or before April 30 annually, the head of the agency (i.e., the Chancellor), submits an *Internal Control Summary and Certification Form* to the Division of Budget to affirm whether or not the University has complied with the six specific requirements of the Internal Control Act as outlined above.

The Internal Control Summary and Certification Form allows agencies to certify to corresponding levels of compliance with each of the Act's requirements. The form is used to provide supporting justification for full or partial levels of compliance. The form can also serve as an agency's compliance plan to identify areas of partial compliance or non-compliance which need to be addressed, including specific timeframes for achieving compliance. The Internal Control Summary and Certification Form requirements are presented to agencies each year in a Budget Bulletin calling for the annual certifications.

The annual Internal Control Summary and Certification Form provides supporting justification for an agency's level of compliance with the requirements of the Internal Control Act and has agencies report on:

1. The internal control review and testing process, high-risk activities and those areas which were reviewed;
2. The significant deficiencies revealed by the review process, summarizing the actions taken to eliminate deficiencies and describing the system used to monitor corrective actions;
3. Education and training provided to keep staff aware of internal controls and to sustain the effectiveness of the internal control program; and,
4. Where appropriate, information on the entity's Internal Audit function, including details on organizational placement, independence and reporting; the qualifications of the Director of Internal Audit; and the processes used by the unit to organize, manage and operate its internal audit activities and processes (e.g., risk analysis, audit planning, work papers, audit committee, continuing professional education, peer review, etc.).

New York City Comptroller's Directive #1 - Financial Integrity Statement and Checklist

The City of New York's Office of the Comptroller releases, on an annual basis, a Comptroller's Memorandum entitled *Directive #1 - Financial Integrity Statement* and its accompanying internal control checklist (*Directive #1 Checklist*) by means of a Comptroller's Memorandum. The Agency Head (i.e., the Chancellor), is required to sign the Financial Integrity Statement, which represents a formal opinion regarding the adequacy of the University's internal control structure. This opinion is supported by the Directive #1 Checklist that the University's community college administrators are required to complete. The Directive #1 Checklist questions represent basic internal control criteria that University's community college manager should follow in order to maintain a reliable and effective internal control system.

New York State Office of the State Comptroller's - Certifying Controls over the Agency's Payment Process

OSC's *Guide to Financial Operations Chapter XII Section 4.D - Certification of Internal Controls over the Payment Process* requires each agency to maintain adequate internal controls over the payment process to support the validity of the agency claim certification for processing payments. In addition, it requires the head of the agency (e.g., the Chancellor) to annually submit on or before April 30, an *internal controls certification form* to the Comptroller certifying that the University has established such a system of internal control over the payment process. This certification requirement is separate and distinct from the NYS Division of Budget's annual Internal Control Summary and Certification.

The CUNY Internal Control Program

The City University of New York's Internal Control Program is designed to ensure that daily operating practices and procedures are sufficient to minimize the possibility of operational failure, overspending, or other actions inconsistent with University policies or violations of law by reviewing, evaluating, and improving the University's existing systems and procedures. The program incorporates the Office of State Comptroller's "Standards for Internal Controls" and the Committee of Sponsoring Organization's (COSO) 2013 Internal Control - Integrated Framework.

The "Four Step Process" was developed by the NYS Division of Budget as a method of evaluating and documenting the system of internal controls which an organization uses to achieve their goals and objectives. CUNY uses the suggested "4 Step" process for reviewing internal controls as the basis for its program and forms. The program consists of four interrelated sections:

o *Identify functions* the primary goal of this step of the internal control process is to develop a campus-wide inventory of program and administrative functions necessary for the University and college departments to carry out its mission. Each of these assessable units will be the subject of a risk assessment. Once the campus inventory of assessable units has been developed, it should be documented;

o ***Conduct Risk Assessments*** A risk assessment is performed by management on each of the assessable units identified in the first step. A risk assessment is a preliminary judgment concerning the existence and adequacy of safeguards or controls now in place. Upon completing a risk assessment, a rating of low, average or high risk is assigned to the assessable unit. These ratings are considered when scheduling internal control reviews. The manager of each assessable unit should be responsible for and participate in each of the unit's risk assessments;

o ***Conduct Internal Control Reviews*** Internal control reviews are detailed examinations of activities to determine whether adequate control measures exist, are implemented, and are effective. This process is conducted through a self-assessment questionnaire and may include a one-on-one discussion with the unit manager and the college Internal Control Officer;

o ***Take Corrective Action*** After reviewing the system design and testing the functioning controls, the reviewer should reach conclusions concerning the effectiveness of the controls. When the reviewer concludes that areas remain where controls do not provide reasonable assurance that a control objective is being met, or that unnecessary controls exist, follow-up actions are required.

Control Self-Assessment of High Risk Areas

Control Self-Assessment (CSA) is a process by which University functional areas, with assistance from the University Office of Internal Control, assess the adequacy of their internal controls and identify opportunities for improvement.

The CSA process involves two key components:

- Department staff members play an active role in assessing their internal controls.
- Department staff members are given the tools to conduct self-audits between Internal Audit visits.

Control Self-Assessment is effective in assessing the control environment, business and financial risk, control activities, and control effectiveness. Although CSA empowers University operating personnel and enhances business partnering between Internal Audit and departmental personnel, it does not eliminate the need for a formal audit.

Our goal is to provide you with information that will allow you to internally assess your operations and determine if your department has reasonable internal controls in place. The Control Self-Assessment (CSA) is a guide to assist with improving internal controls and business practices, so all departments can comply with institutional policies and procedures while limiting the potential for misappropriation of institutional resources. Implementation of the internal controls determined to be necessary upon completion of a CSA will enable you to establish a positive control environment. Ultimately, it is management's responsibility to establish and maintain adequate internal controls.

One requirement of the Internal Control Program is that the college periodically assess campus operations for programs that may be considered "high risk" through one or more combinations of factors. Factors which contribute to a determination of high-risk include, among others, handling a large volume of cash transactions, managing significant institutional resources or assets, administering a large volume of data of a confidential or sensitive nature, or having significant interaction with the public where the risk of institutional exposure is high.

CUNY has identified for all campuses a number of such areas and each college is responsible for identifying any other campus-specific programs and/or functional areas that are also determined to be high-risk.

High Risk Areas

- Procurement
- Accounts Payable
- Travel/Employee Expenses
- Human Resources/Payroll
- Bursar/Cash Management
- Property Management/Inventory
- Information Technology
- Public Safety
- Financial Aid
- Non-Tax Levy Accounts

The University Internal Control Officer will distribute the CSA to the College ICOs as issued. Selected University departments are asked to complete the CSA. The results of the questionnaire will enable University management to:

- Assess the overall internal control environment of the University
- Document each department's internal controls status
- Inform new department heads of their responsibilities related to internal controls
- Identify areas of internal controls weaknesses so that corrective action can be taken.

Internal Control Activities and Best Practices

University employees take pride in their work and want to do the "right thing" but they need to know what is expected of them and have the resources, information, and tools available to allow them to successfully carry out their responsibilities. Our goal is to compile a resource of recognized internal control activities and best practices in managing business risks for creating effective and efficient systems of internal control. It is the clear expectation of the University Office of Internal Control that, absent a valid business reason to the contrary, departments will strive to integrate these practices into their business processes.

Internal Control Types and Activities

Types of Controls:

Preventive controls are proactive in that they attempt to deter or prevent undesirable events from occurring.

Corrective controls are put in place when errors or irregularities have been detected.

Detective controls provide evidence that an error or irregularity has occurred. These controls may also be referred to as *mitigating* controls. They help to reduce risk associated with a failure to implement preventive controls. For example, if properly segregating duties is not possible due to limitations of staffing resources, random or independent reviews of transactions, after-the-fact approvals, or exception report reviews can mitigate the risk exposure.

While preventive controls are preferred, detective controls are still critical to provide evidence that the preventive controls are functioning as intended.

Internal control activities are the practices performed by departments to provide management with reasonable assurance that financial information is timely and accurate, transactions are authorized, valid, complete, that assets are safeguarded and properly accounted for, and that the University complies with all prevailing laws and administrative regulations of the City and State of New York and the Federal government.

The following are descriptions of some of the more commonly used *internal control activities*. This is by no means an exhaustive listing of the alternatives available to management.

Internal Control Activities

Written Policies and Procedures (Preventive)

Management should document business processes, personnel responsibilities, departmental operations, and promote uniformity in executing and recording transactions. Thorough policies and procedures serve as effective training tools for staff and faculty. If written policies and procedures do not exist, are inaccurate, incomplete, outdated, irrelevant, not written succinctly, and/or not communicated; the following could result:

- Inconsistent practices among employees and/or departments

- Processing errors due to a lack of knowledge

- Inability to enforce employee accountability

Written policies and procedures establish management's criteria for executing the University's operations. Developing and documenting policies and procedures is the responsibility of management. Management should therefore:

- Document all significant business practices, processes, and policies;

- Effectively communicate new policies and procedures to personnel;

- Ensure policies and procedures are accurate, complete and current at all times;

- Revise policies and procedures for changes in business processes and policies. This is important when new systems are developed and implemented or other organizational changes occur;

- Communicate significant changes to all affected personnel to ensure they are aware of any revisions to their daily duties and responsibilities; and

- Policies and procedures are only effective if people are aware and understand them.

Proper Approvals, Authorization and Verification (Preventive)

The action of approving transactions should not be taken lightly. An approval indicates that the supporting documentation is complete, appropriate, accurate, and in compliance with University policy and procedures. Unusual items should be questioned.

Persons approving transactions should have the authority to do so and the knowledge to make informed decisions.

Authorization should always be obtained from a higher-level supervisor of the employee. This would include Department Heads, Directors, Vice-Presidents, Deans, etc. who ordinarily would have signatory authority over such transactions. No one should be allowed to approve payments to him/herself or to suppliers and vendors for expenses they have personally incurred on behalf of the University.

Access to confidential information must be relevant to work responsibilities ("need-to-know" access). Authorization and access privileges must be modified or deleted, as appropriate, immediately upon the transfer or termination of employees in order to protect the integrity of the internal control system. Examples of actions to take upon transfer or termination of an employee are as follows:

- Return of keys to buildings, offices, and vehicles.

- Return and cancellation of any University issued credit card (P/Travel/NET).

- Notification to the Public Safety Office relative to building access privileges.

- Notification to the Business/Comptroller's Office of change in signature authority.

- Disable computer access privileges.

Accountability (Detective)

The identity of all individuals involved in a process or transaction should be readily determinable to isolate responsibility for errors or irregularities. This is known as an audit trail and can take the form of signatures, initials, date/time stamps, computer login IDs, or other means of identification. The documents or IT records containing this information must be kept on file and available for examination for a reasonable time period, in line with the record retention policy.

Separation of Duties (Preventive)

No one person should be able to control a transaction or process from beginning to end without intervention or review by at least one other person.

Specifically, an individual should not be in position to initiate, approve, undertake, and review the same action. This principle is not limited to financial activities alone (i.e. processing student grades). Involving two or more people to perform key responsibilities reduces the opportunity for misappropriation of funds or fraud. Examples include:

- *Revenue* – A single person should not handle cash and verify deposits. Ideally three people are needed to properly segregate duties, one person receives the revenue and creates a receipt, another person prepares the deposit, and a third reconciles it to the general ledger monthly. If only 2 are available, the cashier can return the validated deposit slip to the first person to be compared to the receipts generated. If the receipts were for a payment on an account, the deposit process should be separated from posting the payment to the accounts receivable.

- *Expenditure* – One person should not process, approve, and reconcile expenditures. At minimum, the approval and reconciliation duties should be segregated.

- *Payroll* – Ideally, one person should input time, another approve, and a third reconcile. The person who adds new employees on payroll should not also enter and approve hours worked, distribute paychecks (direct deposit should be encouraged), and manage the departmental budget.

In all cases, independent post-transactional review or reconciliations by the person fiscally responsible for the budget should be performed to help achieve greater control.

Reconciliations (Detective)

Monthly reconciliations of the detailed transactions posted to accounts are one of the most important controls that can be performed. These reviews provide a system of checks and balances to detect fraud, theft, inappropriate use of funds, or human error. Additionally, these reviews will assist in assessing the effectiveness and efficiency of business practices.

Fiscal responsibility may be delegated to clerical, faculty, or administrative staff but ultimately is retained by Deans, Directors, and Department Heads who should at minimum:

- Review reconciliations for consistency and reasonableness.

- Ensure reconciliations are timely and complete.

- Follow-up on any questionable items or problems detected.

Overall, the University is very fortunate to have honest, competent, and dedicated employees; however, as in any company mistakes can happen. And while the vast majority of employees are trustworthy, the university must have checks and balances in place to detect the small minority of employees who may not. Management (i.e. Deans, Directors, Managers, Supervisors, etc.) needs to understand that ultimately the responsibility for oversight and review remains with them. Some of the types of fraudulent activity to be aware of include, but are not limited to, the following:

- Creation of fictitious invoices to substantiate fictitious business expenses for reimbursement.

- Use of the University credit card to buy personal items.

- Entry of time into payroll for hours not worked.

- Use of University resources (i.e. supplies, equipment, student labor, etc.) to benefit a private business in which faculty or staff have ownership interest.

- Misappropriation of cash receipts.

Management is responsible for ensuring that routine reviews of financial transactions are adequate to provide reasonable assurance this type of activity is detected on a timely basis. Indication that the reviews have taken place should be documented (i.e. initials or checklist). Any discrepancies should be investigated.

Reconciliations can also serve to provide insight into the pattern of revenues and expenses that may provide opportunities to streamline or improve business processes. Financial activity should be compared on a regular basis to budgeted and/or projected amounts. Variances can indicate changes in the particular business environment, which may warrant changing certain aspects of how business is conducted. Other variances could indicate that processing errors or fraudulent activities are occurring. A variance threshold should be established based on key financial indicators. Variances in excess of the threshold should be investigated.

Security/Safeguarding (Preventive and Detective)

All reasonable efforts should be made to safeguard the physical assets of the organization from the risk of loss or damage. Examples of these assets include:

- Cash, checks, securities.
- Machinery, office equipment, furnishings, vehicles.
- Computer hardware, software, databases.
- Cell phones.
- Important documents, financial transaction records, confidential files.
- Buildings/offices.
- Inventories of goods for resale, tools, supplies.

Accuracy of Data Entry (Preventive and Detective)

Original data entry into production computing systems should be checked, verified, or edited in some way to identify errors to ensure accuracy and reliability of the data. The most appropriate or efficient method will depend on the particular computing system and the type of data. Examples of methods commonly used include:

- Comparison of output reports to original data entry documents.
- Built-in computer system edits to check for "reasonableness" of data in key fields.
- Comparison of batch totals of certain statistical data to output reports of matching statistics.
- Reconciliations.

Best Practices

Best practices are simply the best way to perform a business process. Best practices represent proven methodologies for consistently and effectively achieving a business objective. Best practices are not the definitive answer to a business problem; instead, they are a source of creative insight for business improvement. Adapting best practices to your specific operational needs can substantially affect performance…leading to breakthroughs that save time, enhance quality, lower costs, increase revenue, and improve audit results.

Department managers are strongly encouraged to use the best practices as a tool to evaluate their existing control activities and to make any requisite improvements to their department's internal control system. These best practices can also serve as a resource to departments when developing, or strengthening, written procedures and documentation of their business processes. While all of the best practices listed are "recommended," we recognize that often there is not a "one-size-fits-all" solution.

The following best practices are intended to support and expand upon the internal control framework as presented in the *New York State Office of the State Comptroller's* *"Standards for Internal Controls"*.

Best Practices for Cash Receipts and Revenue

Risks: Misappropriation, unrecorded receipts, fraud

Cash Receipts

Strong internal controls are necessary to prevent mishandling of funds and to safeguard assets. They protect both the university and the employees handling the cash.

Safeguarding Cash

- Restrictively endorse checks immediately upon receipt stating "For Deposit Only – City University/College Name".

- Keep cash/checks in a *locked and secure area* until they can be deposited. Access to the area should be restricted to only designated individuals. If a person with custody responsibilities leaves their position, any keys should be collected and combinations changed. Remember that while cash or checks are in your custody you are responsible for it.

- Make timely deposits. The sooner cash/checks can be deposited the less exposure to theft or loss of funds. Ideally deposits should be made within 24 hours. If amounts are insignificant (less than $100) then deposits can be made weekly.

Recording Cash Receipts

- All cash receipts should be recorded immediately by use of a cash register or other point-of-sale device, data entry into a computing system, pre-numbered receipt book, or handwritten log. Receipts can be in manual or electronic format and should contain the amount received, the name of the payer, purpose of the payment, and its form (cash/ check/credit card).

- Provide a receipt. Ideally receipts should be pre-numbered and two-part. One copy should be provided to the payer while the other copy is kept on file. Total deposits can be verified independently by another person by accounting for each sequentially numbered receipt.

- Cash receipts should not be used for petty cash disbursements, check cashing, making change, or for any personal reasons.

Reconciliation

- Verify the deposit by agreeing the Bursar deposit slip to the general ledger on a monthly basis.

- Cash registers and credit card machines should be balanced daily. Over/short amounts should be monitored.

- A dated and signed record of the reconciliation should be maintained.

Segregation of Duties

No one person should be allowed to collect, handle or transport and deposit checks/currency without some additional control feature to ensure that all funds are accounted for. Examples of such controls are as follows:

- The person collecting and recording the receipt should not be the same as that making the deposit. Additionally, a person independent of recorder and depositor responsibilities should reconcile the deposit to the general ledger. If there are only one or two people in the department, a review by management of the reconciliation can provide a compensating control.

- When cash or checks are received regularly in the mail, if feasible, two persons should be present when the mail is opened. One person should total and record the remittances (log). The other, should prepare the deposit slip and forward it with the cash/checks to the Bursar Office. The deposit slips should be reconciled by a third person to the general ledger.

- Keep transfers of cash from person to person to a minimum. Accountability is lost when several people handle cash before it is deposited. If transfers must take place be sure to document it. If you are the transferor you should get a receipt, if you are the transferee you should verify what you are receiving before you provide a receipt. Use of a drop-off/pick-up log can be beneficial when transporting deposits.

Fees and other Revenues

Use an accounts receivable account to process billing and collection for routine revenue activities. Internal controls surrounding this type of activity include:

- Maintain a subsidiary ledger of customer accounts, including all invoices and payments.

- Invoices should be pre-numbered.

- The total of all payments should be agreed to the associated revenue accounts at least monthly.

- The accounts receivable should be aged and reviewed monthly for past due revenues.

- All delinquent accounts should be followed up for collection.

- The subsidiary ledger should be agreed to the associated accounts receivable account monthly.

- All credits, adjustments, refunds should be properly documented and authorized by management prior to entry into the receivable records.

- Accounts to be written off should be properly approved by management.

- Duties should be segregated, in that the person responsible for billing does not also collect the receipts.

Bank Accounts

The opening of any University bank account requires proper approval from the Office of the University Controller (OUC).

- No individual school, college or department bank accounts are permitted without authorization from the College Business Office.

- Bank accounts for outside clubs or organizations cannot use the University's or College's tax ID number.

Best Practices for Procurements and Expenditures

Risks: Personal Charges, Fraud, Kickbacks, Policy Violations, Duplicate Charges, Misappropriations

General Expenditures

Disbursements should be handled in a manner that ensures proper use of funds and appropriate accounts charged. The disbursement should be properly authorized and in compliance with applicable policy, law or regulations.

- Purchases should be coordinated through the Purchasing Office to obtain competitive bidding which ensures best pricing and products.

- Use vendors with whom the University has discount agreements or are recommended by Purchasing.

- Ensure approvals are from an appropriate level and are someone of higher authority and other than the preparer.

- Separate authorization and reconciliation duties.

- Ensure the person responsible for account reviews reconciles the transactions to supporting documentation.

- Personal items should not be purchased even if the employee will reimburse.

- Sales tax should not be paid.

- Use the University credit card for ease of processing transactions.

University Credit Card Purchases

The use of credit cards is encouraged due to the convenience and enhancement of operational efficiency. The use of credit cards has also shifted a degree of purchasing authority from Purchasing to the many departments and units across the University community. At City University, departments and cardholders have been assigned some basic responsibilities to control, monitor, and manage the use of the cards as follows:

- Cardholders are responsible for the safekeeping of the cards, and cards should not be used by anyone other than the designated cardholder. Cards are to be used by individuals and not groups.

- Monthly reconciliations should be performed to support the statements with receipts that clearly document the purpose of the expense. Sufficient documentation should be attached and filed for easy reference.

- The person approving the expenditures should be someone other than the cardholder and an authorized account signer. The approver should be at a higher level of authority than the cardholder.

- The pre-set per transaction spending limits may not be exceeded under any circumstances. Do not split transactions to avoid this limit or your card could be revoked.

- Cardholders are responsible to obtain itemized transaction receipts for ALL transactions.

- Card users are responsible to make certain sales tax is not charged.

- Report lost or stolen cards immediately.

- Cardholders may not use the cards for personal use.

- Procedures should be in place to disable cards immediately upon termination or separation of employment, including notifying the Administrator of the Credit Card Program at the College.

Travel

The policy and procedures surrounding travel are discussed in detail in the State of New York Travel Manual for senior colleges and City of New York Directive 6 for community colleges. **ALL** travel expenses are required to have supporting documentation including itemized receipts outlining the date, place, amount, and specific business purpose. There are a few additional considerations:

- Consideration should be given to using the University Travel/NET card.

- It is important to mention that the travel can be recognized by the IRS as compensation if certain criteria are not met.

- Spouse/guest travel is generally unallowable unless paid for separately.

Petty Cash (Imprest Funds)

The University credit card can be used to purchase many of the items a petty cash fund was traditionally used for. If there is still a need for a petty cash or imprest fund account, then keep the following in mind for good internal control practices:

- Only one individual should have access and responsibility for the fund, with a back-up designated on an as needed basis.

- Funds should be on the books. This means the funds need to be established through the Comptroller's Office and assigned an account number.

- Someone other than the custodian should periodically count and verify the fund balance. The total of the cash plus the receipts plus outstanding reimbursements should equal the original amount of the fund.

- Do not use the funds for personal business, including loans, expenses or the cashing of checks.

- Ensure original receipts are maintained and the explanation of the business purpose documented for all expenditures.

- Periodically (at least monthly) submit all receipts for reimbursement. The reimbursement should be reviewed by a supervisor for propriety prior to submission to the Comptroller's Office.

- Keep the fund physically secured at all times.

- Consideration should be given to closing the petty cash fund if there is no longer a need for it. University credit cards can be used as an alternative.

Best Practices for Payroll

Risks: Fictitious Employees, Overpayments, Excessive Leave, Unauthorized Hours

Payroll

- Payroll transactions should be properly recorded and authorized.

- Paychecks should be appropriately distributed and employees validated.

- Payroll timekeeping, input, and authorization functions should be segregated.

- Specifically, duties should be adequately segregated; meaning, payroll should be approved by someone other than the person responsible for inputting the information. Also, someone other than the person who inputs or authorizes payroll should distribute the payroll checks. A person independent of input and authorization responsibilities should review labor distribution reports monthly. This review should be documented via initials.

- Timesheets should be used for all non-exempt employees to record the time worked and be approved by a supervisor.

- Exempt and non-exempt employees need to document and report sick and annual time as unworked time to the Payroll Office.

- All unclaimed paychecks should be returned to the Payroll Office if not picked up within 30 days.

- Physical checks should be locked in a secure area until distributed.

- Use a distribution log to provide accountability of the whereabouts of a check.

- Encourage direct deposit of checks.

- Terminated employees should be reported to HR/Payroll immediately.

Best Practices for Fixed Assets and Inventory

Risks: Theft, Improper Recording of Assets, Inaccurate Inventories

Fixed Assets and Major Equipment Inventory

City University defines "major equipment" as equipment with an expected useful life of more than one year and a value greater than or equal to $5,000. Property Management is charged with the recordkeeping of all fixed assets, whether the purchase is with University or sponsored programs funds.

Data such as description, cost, age, depreciation, location and custody is maintained in the CUNYFirst Asset Management System. Individual departments/schools/colleges are responsible for the physical safeguarding of the assets, tracking of an asset's movement, or disposal. Specifically the department/school/college should:

- Ensure capitalized equipment has a tag issued by Property Management.

- Complete the inventory reports sent annually listing capitalized equipment. A physical inventory is required to be taken to validate accuracy of system records. Any differences should be investigated, documented and reconciled.

- The inventory should be conducted by someone other than the person responsible for purchasing the assets.

- Property Management should be notified of any updates that need to be made to the inventory system by returning the inventory report, signed by the Dean, Director or Department Head.

- Fill out appropriate form that acknowledges receipt and responsibility for equipment that is being removed from University premises.

- Notify Property Management if capitalized equipment is moved to another location on campus. Provide the tag number, previous location and the current location so the inventory records can be undated accordingly.

- Contact Property Management to determine the appropriate method for disposing of surplus equipment.

- University property should be collected upon separation of employment.

Sensitive Items (Portable Equipment)

OIAMS strongly encourages departments to keep track of equipment that falls under the $5,000 capitalization threshold that may be easily misappropriated. Examples include: laptops, cameras, video cameras, iPads, tablets, and cell phones. Best business practice should include maintenance of a department inventory list. The list should at minimum include a description of the property with an identifying factor such as a serial number and the employee who it is assigned to. Additionally, a physical inventory should be performed annually.

Management may decide to not implement certain best practices because they are not applicable, they are redundant (due to other compensating control activities), or not cost beneficial. Managers should document these decisions and periodically review them to ensure they have not become invalidated by changes in the department's operating environment.

Appendix A – Additional Internal Control Guidance & Resources

The City University of New York is committed to maintaining a strong system of internal control as a business best-practice. Our decentralized environment at the University requires that every employee with fiscal responsibility be fully aware of our business operating environment and internal controls requirements. Each individual within a unit should be cognizant of proper internal control procedures associated with their specific job responsibilities and is responsible for complying with internal controls. The Office of Internal Control strongly recommends all University employees become familiar with the wealth of resources found on the following websites:

Committee of Sponsoring Organizations of the Treadway Commission (COSO)
http://www.coso.org/
Internal Control – Integrated Framework

New York State Office of the State Comptroller
http://osc.state.ny.us/agencies/ictf/index.htm
Standards for Internal Control in New York State Government

The New York State Office of the State Comptroller has also developed an online PowerPoint training tool reviewing all aspects of a good internal control system.

New York City Comptrollers' Office
http://comptroller.nyc.gov
Directive 1 - Principles of Internal Control

New York State Internal Control Association
http://www.nysica.com

The University Internal Control Office
The City University of New York
230 West 41ˢᵗ Street, 11th Floor
New York, New York 10036
Phone: (646) 664-3090
Fax: (646) 664-3219

August 2016