THE NEW YORK STATE INTERNAL CONTROL ACT

INTERNAL CONTROL REVIEW

COMPONENT AND PRINCIPLE EVALUATION GUIDE

MAY 2018

TABLE OF CONTENTS

ACKNOWLEDGMENTS

DISCLAIMER

This guide is designed to provide you with the knowledge necessary to apply the Committee of Sponsoring Organizations of the Treadway Commission's (COSO) *Internal Control – Integrated Framework* (COSO Framework). Following this guide will help you review and evaluate your agency's internal control system, but it cannot guarantee an unqualified audit opinion will be achieved. Some language has been changed and examples have been added to aid you in applying the components, principles, and points of focus to state government operations. These examples are for illustrative purposes to guide you in interpreting a component, principle, or point of focus. They are not intended to be an all-inclusive list. As you apply this guide, the term 'agency' can be substituted with public authority, university, board, commission, council, etc. as it applies to your specific government entity.

In determining whether a component is present and functioning, management needs to determine to what extent relevant principles are present and functioning. A principle being present and functioning does not imply that the agency strives for the highest level of performance in applying that particular principle.   Management exercises judgment in balancing the cost and benefit of designing, implementing, and conducting internal control.

Internal control, no matter how well designed, implemented, and conducted, can provide only reasonable assurance to management and the Board of Directors of the achievement of an agency's objectives. The likelihood of achievement is affected by limitations inherent in all systems of internal control. These include the realities that human judgment in decision making can be faulty, external events outside the agency's control may arise, and control breakdowns can occur. In addition, the potential exists for controls to be circumvented through collusion or by management override.

LEGAL FRAMEWORK

The *New York State Governmental Accountability, Audit and Internal Control Act* (Internal Control Act) requires state agencies and other organizations to promote and practice good internal controls. New York State Finance Law requires the State Comptroller to issue internal control standards for state agencies, public authorities, and other organizations.

INTERNAL CONTROL ACT

The 1987 Internal Control Act requires state agencies to establish and maintain a system of internal controls and a program of internal control review for the agency.

'State agency' as defined by the Internal Control Act is "any state department, state university of New York, city university of New York, board, bureau, division, commission, committee, council, office or other governmental entity performing a governmental or proprietary function for the state, or any combination thereof, except any public authority or public benefit corporation, the judiciary or the state legislature."

The Internal Control Act requires state agencies to:

1. Establish and maintain guidelines for a system of internal controls that are in accordance with internal control standards.

2. Establish and maintain for the agency a system of internal controls and a program of internal control review.

3. Make available to each officer and employee of the agency a clear and concise statement of the generally applicable management policies and standards with which the officer or employee of such agency shall be expected to comply.

4. Designate an internal control officer, who shall report to the head of the agency, to implement and review the internal control responsibilities established.

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

6. Periodically evaluate the need for an internal audit function.

BUDGET POLICY & REPORTING MANUAL ITEM B-350

The New York State Division of the Budget's Budget Policy & Reporting Manual Item B-350 (Item B-350) requires the head of each covered agency to annually certify compliance with the Internal Control Act and report the internal control activities undertaken by the agency during the preceding fiscal year. Internal Control Summary and Certification forms are due to the Division of the Budget on or before each April 30th.

STANDARDS FOR INTERNAL CONTROL IN NEW YORK STATE GOVERNMENT

Item B-350 states that the system of internal control should be developed using the COSO Framework adopted in the *Standards for Internal Control in New York State Government*, promulgated by the Office of the NYS Office of the State Comptroller (OSC Standards).

The OSC Standards are based in part on the work of those advocated by leading authorities in the field of internal controls, such as COSO, the United States Government Accountability Office (GAO), and other professional organizations.

The March 2016 OSC Standards incorporate the 2013 update to the COSO Framework and the 2014 update to the GAO's *Standards for Internal Control in the Federal Government* (Green Book) but adapt them to better fit the NYS government structure.

DEFINITION OF INTERNAL CONTROL

Internal control is defined as a process, effected by an agency's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance. It is the integration of the activities, plans, attitudes, policies, systems, resources and efforts of the people of an agency working together to achieve its mission.

REQUIREMENTS FOR EFFECTIVE INTERNAL CONTROL

An effective system of internal control provides reasonable assurance of achievement of an agency's objectives. Internal controls are the first line of defense and the best mechanism an agency has to safeguard its assets and resources, even though they can provide only reasonable – not absolute assurance. An effective system of internal control reduces, to an acceptable level, the risk of not achieving an objective. It requires that:

- each of the five components of internal control and relevant principles is present and functioning, and

- the five components are operating together in an integrated manner.
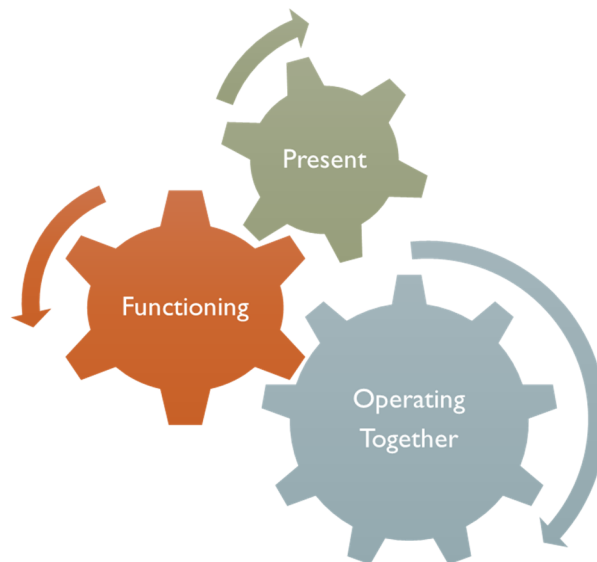
ROLES AND RESPONSIBILITIES

Every member of an agency has a role in effecting the system of internal control. Collectively, they contribute to providing reasonable assurance that agency objectives are achieved.

BOARD OF DIRECTORS

* This role becomes the agency's top executive (commissioner) if the agency does not have a Board of Directors.

1. Should discuss with agency leadership the state of the agency's system of internal control and provide oversight as needed.
2. Needs to establish its policies and expectations of how members should provide oversight of the agency's internal control system.
3. Should be apprised of risks to the achievement of the agency's objectives, the assessments of internal control deficiencies, and how management assesses the effectiveness of internal controls.
4. Should challenge agency leadership; ask questions, as necessary; and seek input and support from internal control officer, internal auditors, external auditors, and others.

AGENCY LEADERSHIP

1. Should create a positive control environment that supports strong governance, ethical values, integrity, competence, morale, and structure throughout the agency.
2. Should set the agency's expectation for internal controls, ensuring management is aware of those expectations, and evaluating management's effectiveness at maintaining and supporting the system of internal controls.
3. Should focus their monitoring activities on the major divisions of the agency and place emphasis on monitoring the achievements of the agency's goals.

DIRECTORS AND MANAGERS

1. Should ensure employees have the necessary skills, knowledge, and training to reasonably ensure they can carry out their work.
2. Should develop internal controls for compliance with agency policies and procedures as well as applicable laws, rules, and regulations.
3. Should periodically review their processes and procedures to ensure that proper internal controls are in place and being followed.
4. Need to introduce new controls and strengthen internal controls when weaknesses or opportunities for improvement are identified.
5. Should focus monitoring activities on assessible units with emphasis on achieving the agency's goals.

SUPERVISORS

1. Should ensure internal controls are operating as intended for compliance with agency policies and procedures as well as applicable laws, rules, and regulations.
2. Need to implement new internal controls or strengthen existing controls when weaknesses or opportunities for improvement are identified.
3. Should monitor activities and transactions in their unit to ensure that staff members are performing their assigned responsibilities, control activities are functioning properly, the unit is accomplishing its goals, the unit's control environment is appropriate, communication is open and sufficient, and risks and opportunities are identified and properly addressed.

STAFF

1. Should have an understanding of internal controls and control concepts supporting the system of internal controls within their unit.
2. Should comply with agency policies and procedures as well as applicable laws, rules, and regulations.
3. Should be focused on monitoring their own work to ensure it is done properly.
4. Should correct errors identified before work is referred to higher levels for review.

INTERNAL CONTROL OFFICER

1. Responsible for establishing and maintaining an internal control review program to ensure internal controls are in place and for promoting compliance with agency policies; procedures; and applicable laws, rules, and regulations.
2. Responsible for educating and training agency staff on internal controls and control concepts.

INTERNAL AUDIT

1. Responsible for assessing the adequacy and effectiveness of agency internal controls and reporting weaknesses and opportunities for improvement to management as they are identified.

OBJECTIVE SETTING

Agency leadership, with board or commissioner oversight, sets objectives that align with the agency's mission, vision, and strategies. The COSO Framework groups agency objectives into three categories: operations, reporting, and compliance.

OPERATIONS OBJECTIVES

Operations objectives relate to the effectiveness and efficiency of operations, including operations and financial goals.

These objectives promote orderly, economical operations to produce quality products and services consistent with the agency's mission. They also safeguard resources against loss due to fraud, waste, abuse, errors, and mismanagement.

REPORTING OBJECTIVES

Reporting objectives pertain to the reliability of reported information in accordance with professional standards; applicable laws, rules, and regulations; and control agency expectations.

Reports may be financial or nonfinancial reports of operations for use by the agency, its stakeholders, or other external parties. These objectives may encompass reliability, timeliness, transparency, or other terms set forth by regulators, recognized standard setters, or agency policies.

COMPLIANCE OBJECTIVES

Compliance objectives incorporate adherence to requirements of applicable laws, rules, regulations, contracts, and management directives. Management determines which laws, rules, regulations, and contracts apply to agency operations.

Run operations efficiently and effectively

Report reliable information about operations

Comply with applicable laws, rules and regulations

SUITABILITY AND RELEVANCE OF COMPONENTS AND PRINCIPLES

The COSO Framework views all five components and seventeen principles of internal control as suitable and relevant to all entities. Principles have a significant bearing on the presence and functioning of an associated component. If management determines a principle is not suitable or relevant, management must support its determination with the rationale of how, in the absence of that principle, the associated component can be present and functioning. Points of focus are important characteristics of principles; management may determine that some of the points of focus are not suitable or relevant and may identify and consider others based on specific circumstances of the agency. Management does not need to separately assess whether points of focus are in place.

CONTROL ENVIRONMENT

The control environment is the set of standards, processes, and structures that provide the basis for carrying out internal control across the agency. Agency leadership establishes the tone at the top regarding the importance of internal control. Management reinforces these expectations at the various levels of the agency.

PRINCIPLE 1
THE AGENCY DEMONSTRATES A COMMITMENT TO INTEGRITY AND ETHICAL VALUES.

The commissioner, agency leadership, and management at all levels of an agency demonstrates a commitment to integrity and ethical values through its commitment to competence all the while exercising oversight of the development and performance of internal control and enforcing accountability.

PRINCIPLE 2
THE BOARD OF DIRECTORS DEMONSTRATES INDEPENDENCE FROM MANAGEMENT AND EXERCISES OVERSIGHT OF THE DEVELOPMENT AND PERFORMANCE OF INTERNAL CONTROL.

The agency commissioner (or Board of Directors where appropriate) accepts oversight responsibility for agency leadership's design, implementation, and conduct of internal control. The commissioner should ask probing questions of agency leadership, and take commensurate actions.

PRINCIPLE 3
MANAGEMENT ESTABLISHES, WITH BOARD OVERSIGHT, STRUCTURES, REPORTING LINES, AND APPROPRIATE AUTHORITIES AND RESPONSIBILITIES IN THE PURSUIT OF OBJECTIVES.

Agency leadership establishes, with agency commissioner (or Board of Directors where appropriate) oversight, multiple levels of the organizational structure in which the agency's plans are carried out. Agency leadership is responsible for organizing the agency's authority and responsibilities among

various functions in the pursuit of objectives. As such, management ensures that reporting lines throughout the agency are clearly defined, appropriate, and are communicated across all levels of the agency.

PRINCIPLE 4

THE AGENCY DEMONSTRATES A COMMITMENT TO ATTRACT, DEVELOP, AND RETAIN COMPETENT INDIVIDUALS IN ALIGNMENT WITH OBJECTIVES.

The agency demonstrates a commitment to attract, develop, and retain competent individuals by establishing appropriate human resource policies and practices that reflect a commitment to competence necessary to support the achievement of objectives. The agency at all levels evaluates competence, and acts as necessary to address deficiencies. Employees should have adequate resources, such as equipment, software, procedure manuals, as well as the tools and support they need to perform their jobs.

PRINCIPLE 5

THE AGENCY HOLDS INDIVIDUALS ACCOUNTABLE FOR THEIR INTERNAL CONTROL RESPONSIBILITIES IN THE PURSUIT OF OBJECTIVES.

Agency leadership should assess whether internal control responsibilities are understood and adhered to by staff. Actions should be taken to hold individuals accountable for nonfulfillment of their internal control responsibilities with corrective action as necessary and recognition given for the fulfillment of their internal control responsibilities.

RISK ASSESSMENT

Risk assessment involves a dynamic and iterative process for identifying and assessing risks to the achievement of objectives, and forms a basis for determining how risks should be managed. Management should provide guidance throughout the agency to help employees assess the level and the kinds of risk that are acceptable and not acceptable.

PRINCIPLE 6

THE AGENCY SPECIFIES OBJECTIVES WITH SUFFICIENT CLARITY TO ENABLE THE IDENTIFICATION AND ASSESSMENT OF RISKS RELATING TO OBJECTIVES.

The agency's mission, strategic plan, and performance goals all drive management to define specific, measurable, and understandable objectives and to prioritize them by importance based on internal and external factors. The organizational structure, as well as individual responsibilities of staff, assist in the accomplishment of the design of internal controls that address related risks.

PRINCIPLE 7

THE AGENCY IDENTIFIES RISKS TO THE ACHIEVEMENT OF ITS OBJECTIVES ACROSS THE AGENCY AND ANALYZES RISKS AS A BASIS FOR DETERMINING HOW THE RISKS SHOULD BE MANAGED.

Once objectives are identified within all levels of an agency, identifying risk, both internal and external, is a key component in developing and adjusting internal controls. Risks are associated with specific functions, objectives, and units across all levels of staff within an agency. Risk exposure involves people (hiring, training, ethics, organizational structure), processes (policies, procedures, monitoring), systems (hardware, software, programming, development), and external events (political, legal, natural disaster). These risks could impede the effectiveness and efficiency of the agency's operations. Understand the impact and likelihood of an unfavorable occurrence, the nature of the risk, and if possible quantify the significance and management's response to the occurrence.

PRINCIPLE 8

THE AGENCY CONSIDERS THE POTENTIAL FOR FRAUD IN ASSESSING RISKS TO THE ACHIEVEMENT OF OBJECTIVES.

Fraud can exist either as an intentional act or omission of information intended to deceive, resulting in the victim suffering and the perpetrator gaining. Understand the risk types (fraudulent financial reporting, asset misappropriation and corruption), risk factors (incentives, opportunity, attitudes/rationalization) and response needed (significance, impendence in achieving objectives).

PRINCIPLE 9

THE AGENCY IDENTIFIES AND ASSESSES CHANGES THAT COULD SIGNIFICANTLY IMPACT THE SYSTEM OF INTERNAL CONTROL.

Risk needs to be evaluated continually due to internal and external changes, and should be part of the agency's risk assessment process. Revisiting the what, who, when and how as well as the risk exposure of people, processes, systems, and external events, all assist in responding timely to change. Focus on lessening or eliminating the potential negative impact to the internal controls design, implementation, and operating effectiveness. Additionally, new risks should be identified and addressed timely.

CONTROL ACTIVITIES

Control activities are the actions established through policies and procedures that help ensure that management directives to mitigate risks to the achievement of objectives are carried out. Control activities are performed at all levels of the agency and at various stages within business processes. They may encompass a range of manual and automated activities, including both preventive and detective controls.

PRINCIPLE 10

THE AGENCY SELECTS AND DEVELOPS CONTROL ACTIVITIES THAT CONTRIBUTE TO THE MITIGATION OF RISKS TO THE ACHIEVEMENT OF OBJECTIVES TO ACCEPTABLE LEVELS.

Control activities are the policies, procedures, techniques, and mechanisms that enforce management's directives to achieve the agency's objectives and address related risks. Control activities can be either preventive or detective and can be implemented in either an automated or a manual manner. Management establishes control activities that are effective and efficient and contribute to the mitigation of risks. When designing and implementing control activities, management strives for the maximum benefit at the lowest possible cost.

PRINCIPLE 11

THE AGENCY SELECTS AND DEVELOPS GENERAL CONTROL ACTIVITIES OVER TECHNOLOGY TO SUPPORT THE ACHIEVEMENT OF OBJECTIVES.

Management designs the agency's information system to obtain and process information to meet each unit's information requirements and to respond to the agency's objectives and risks. Information technology control activities can be categorized as either general or application controls. These controls are interrelated; general controls support the functioning of application controls, and both types are needed to ensure complete and accurate information processing. While some of the control activities relating to information technology are the responsibility of specialized information technology staff, other control activities are the responsibility of the agency and its employees.

PRINCIPLE 12

THE AGENCY DEPLOYS CONTROL ACTIVITIES THROUGH POLICIES THAT ESTABLISH WHAT IS EXPECTED AND PROCEDURES THAT PUT POLICIES INTO ACTION.

A policy is a guiding principle, set by management, used to establish direction in an agency. Management documents, in policies for each assessable unit, its responsibility for an operational process's objectives; how it addresses related risks; and control activity design, implementation, and operating effectiveness. Management makes those policies available across the agency. A procedure is a series of documented steps to be followed, as a consistent and repetitive approach, to accomplish an objective. Each assessable unit documents procedures, in the appropriate level of

detail, to allow management to effectively monitor the control activity. Procedures should be a clearly stated, centralized, controlled, up-to-date guide of operations. Management periodically reviews policies, procedures, and related control activities for continued relevance and effectiveness in achieving the agency's objectives or addressing related risks.

INFORMATION AND COMMUNICATION

Information is necessary for the agency to carry out internal control responsibilities in support of the achievement of its objectives. Communication occurs internally and externally and provides the agency with the information needed to carry out day-to-day controls. Communication enables personnel to understand internal control responsibilities and their importance to the achievement of objectives.

PRINCIPLE 13
THE AGENCY OBTAINS OR GENERATES AND USES RELEVANT, QUALITY INFORMATION TO SUPPORT THE FUNCTIONING OF INTERNAL CONTROL.

Management uses relevant and high-quality information to make informed decisions and to evaluate the agency's performance in achieving key objectives and addressing risks. Achieving the right balance between the benefits and the costs to obtain and manage information and information systems is a key consideration in establishing an information system that meets the agency's needs. Information is received from a variety of sources and forms.

PRINCIPLE 14
THE AGENCY INTERNALLY COMMUNICATES INFORMATION, INCLUDING OBJECTIVES AND RESPONSIBILITIES FOR INTERNAL CONTROL, NECESSARY TO SUPPORT THE FUNCTIONING OF INTERNAL CONTROL.

Complete and accurate information should be communicated timely, in a usable form, to facilitate informed decision making and completion of essential internal control responsibilities. Information should travel in all directions (across, up, and down an agency) to ensure that all members of the agency are informed and that decisions and actions are communicated and coordinated. A good system of communication is essential for an agency to maintain an effective system of internal control.

PRINCIPLE 15
THE AGENCY COMMUNICATES WITH EXTERNAL PARTIES REGARDING MATTERS AFFECTING THE FUNCTIONING OF INTERNAL CONTROL.

Open external communication channels disseminate important information concerning the entities objectives to partners, customers, regulators, financial analysts, government entities, and others.

This communication is separate and distinct from external reporting. The agency develops and implements controls that facilitate external communication including procedures to obtain or receive information from external parties to share within the agency to use in achieving its objectives.

MONITORING ACTIVITIES

Monitoring is the ongoing review, or separate evaluation, of an agency's activities and transactions to assess the quality of performance over time and to determine whether procedures are effective. Ongoing evaluations are built into the business process at different levels to provide timely information. Separate evaluations are performed periodically to confirm ongoing evaluation's conclusions.

PRINCIPLE 16
THE AGENCY SELECTS, DEVELOPS, AND PERFORMS ONGOING AND/OR SEPARATE EVALUATIONS TO ASCERTAIN WHETHER THE COMPONENTS OF INTERNAL CONTROL ARE PRESENT AND FUNCTIONING.

Management monitors the internal control system through ongoing monitoring and separate evaluations. Ongoing monitoring are routine operations, built into business processes performed continually, on a real-time basis, and adjusted to changing conditions. They are generally performed by line operating or functional managers who are competent and have sufficient knowledge to understand what is being evaluated. Separate evaluations are periodic assessments of the agency's performance compared to established expectations or measurement standards. They can be accomplished through self-assessment or independent review by objective management personnel, internal audit, or external parties. The scope and frequency of separate evaluations is a matter of management judgment.

PRINCIPLE 17
THE AGENCY EVALUATES AND COMMUNICATES INTERNAL CONTROL DEFICIENCIES IN A TIMELY MANNER TO THOSE PARTIES RESPONSIBLE FOR TAKING CORRECTIVE ACTION, INCLUDING SENIOR MANAGEMENT AND THE BOARD OF DIRECTORS, AS APPROPRIATE.

Personnel may identify internal control issues while performing their assigned internal control responsibilities, monitoring activities, or separate evaluations. Communicating internal control deficiencies to the right parties is critical. Personnel communicate these issues internally to the person in the key role responsible for the internal control and, when appropriate, to at least one level of management above that individual. Management evaluates and documents internal control issues and determines appropriate corrective actions. Management, with oversight from the Board of Directors as appropriate, monitors the status of remediation efforts so that they are completed timely.
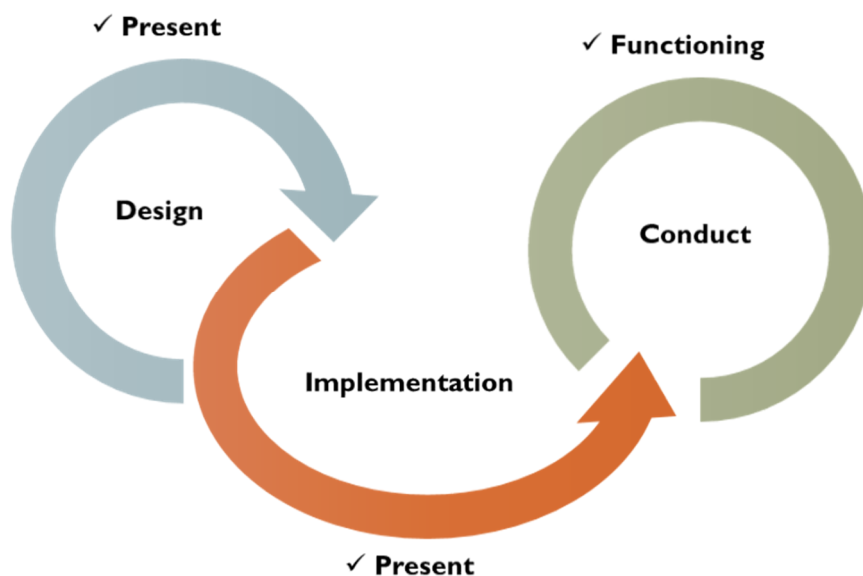
PRESENT AND FUNCTIONING

In determining whether a component is present and functioning one needs to determine to what extent relevant principles are present and functioning. A principle being present and functioning does **not** imply that the agency strives for the highest level of performance in applying that particular principle. Rather, management exercises judgment in balancing the cost and benefit of designing, implementing, and conducting internal control. The determination of controls selected to mitigate the identified risks is subject to management's judgment and risk tolerance.

PRESENT

The determination that components and relevant principles <u>exist in the design and implementation</u> of the system of internal control to achieve agency objectives. Persuasive evidence must exist that proves controls are selected and developed to effect the components and related principles. When evaluating the design of an internal control, management determines if controls individually, and in combination with other controls, are capable of achieving an objective and addressing related risks. The persuasive evidence should be kept and made available upon audit.

FUNCTIONING

The determination that components and relevant principles continue to <u>exist in the conduct</u> of the system of internal control to achieve agency objectives. Persuasive evidence must exist that proves controls are deployed to effect the components and related principles. The persuasive evidence should be kept and made available upon audit.

EXAMPLES OF PRESENT AND FUNCTIONING

Provided below are illustrative examples of controls to effect a principle, ways to determine if the control exists in the design and implementation of the system of internal control, and potential tests that can be conducted to determine if the control exists in the conduct of the system of internal control. Supporting documentation of the presence and functioning of controls should be kept and made available upon audit.

PRINCIPLE	PRESENT	FUNCTIONING
1. The agency demonstrates a commitment to integrity and ethical values.	• The agency establishes and publishes a code of ethics and code of conduct. • Agency Ethics Officer tracks and conducts ethics training. • Agency Ethics Officer contact information is made available to all staff. • Hotline(s) is available to employees, customers, vendors, and the public to report improper use information.	• The code of ethics and code of conduct are distributed and reinforced by management. A copy of the documents is available to all staff. • Ethics training is targeted, on-going, and tailored to the needs of each separate group within the agency. • Ethics Officer maintains an intranet site with clearly posted contact information and resources, including templates for various requests. • Hotline information is available to all staff, external customers and public. Information received from hotline is reviewed and acted upon in a timely fashion.
2. The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	• The agency commissioner, or Board of Directors as appropriate, reviews the assessment of risks including potential impacts of changes, fraud and management override. • Approving and demonstrating agency value statements. • Having an open attitude to internal and external audits and other regulatory authorities. • Supporting internal control self-evaluations and periodic assessments on internal controls with identification of deficiencies and appropriate corrective actions. • Receiving and reviewing reports on monitoring activities identifying exceptions to key controls most importantly actions that override controls and justification for such actions. • Encourages a commitment to excellence and respect for authority.	• The agency commissioner appropriately questions and reacts to risks identified, including developing high-level policy to address risk. • Documentation of the approval of agency value statements. Communication of the value statements. • Agency leadership or board meeting agenda/minutes where internal and external audits are discussed. • Agency cooperation with regulatory authorities and audits conducted. • Agency leadership participates in internal control self-evaluations, internal control certifications and assessments and holds senior management responsible for such. • Date and sign-off on monitoring activity reports. • Verbal or written communication encouraging a commitment to excellence and respect for authority. • Management overrides are tracked and reported.

PRINCIPLE	PRESENT	FUNCTIONING
3. Management establishes - with board oversight - structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	• Formal, documented organization structure. • Units are established around functional responsibilities of agency. • Management also considers the agency's overall responsibilities to external stakeholders. • Management considers conflict of interest inherent in the execution of responsibilities across the agency and its outsourced service providers.	• Current organization charts are reviewed and approved by management and made available to all agency staff. • Management establishes reporting lines within an organizational structure so that units can communicate the quality information necessary for each unit to fulfill its overall responsibilities. • Management establishes reporting lines that allow the agency to both communicate and receive information from external stakeholders. • Management promotes, establishes and monitors the agency's values. • Ensures that outsourced service providers are aware of and follow agency policies and procedures.
4. The agency demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	• Establishing levels of knowledge and skill required for every position or class of positions. • Planning and preparing for succession. • Agency has a business continuity plan for key processes and key positions. • Agency administers mandatory training courses and supports continuous training and development of staff.	• Hiring and promoting only those with the required knowledge and skills. • Verifying the qualifications of job candidates. • Developing contingency plans for the assignment of responsibilities when employees change positions or leave the agency. • The business continuity plan is updated regularly and tested annually. • Management ensures all mandatory training courses are completed. • Agency tracks appropriate continuous training directed toward current jobs as well as future development of staff.
5. The agency holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	• All levels of employees are responsible for knowledge of risk associated with their job duties. • Management establishes performance expectations throughout the agency. These expectations incorporate achieving performance measures and complying with internal control responsibilities. • Management provides employees with a copy of the agency's code of conduct.	• Job duties clearly outline internal control responsibilities, are documented, and periodic job reviews are performed to provide feedback, training, etc. • The agency holds individuals accountable for performance measures and internal control responsibilities. • The agency periodically evaluates performance measures for suitability and relevance. • Management reviews employees' confirmations to assess whether standards of conduct are understood and adhered to by staff across the agency.

PRINCIPLE	PRESENT	FUNCTIONING
6. The agency specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	• Agency has a process for identification of major functions, objectives, associated risks, controls, and testing of those controls. • Agency documents a strategic plan that includes its objectives (mission, vision, goals, strategic priorities). • Agency reporting submissions to State and Federal oversight agencies are accurate and timely. • Management establishes objectives considering the agency's established risk tolerance.	• Major functions, objectives, associated risks, controls are documented and reviewed for accuracy as needed. • Agency communicates the strategic plan, and makes it available, to all staff. • Functional objectives align with agency strategic plan. • Objectives are specified with sufficient clarity. • Compliance levels drive management's actions and set the tone for the agency.
7. The agency identifies risks to the achievement of its objectives across the agency and analyzes risks as a basis for determining how the risks should be managed.	• Management has a process to identify risks to the agency's mission. • Functional managers have a process to identify risks to the achievement of functional objectives. • An individual, or Internal Control Officer, is responsible for overseeing the annual review and management of the risk assessment process.	• Risk assessment process is performed annually, and updated as risks change in between assessment periods, with issues evaluated that could impact the effectiveness and efficiency of the agency. • Annual review of risk and understanding of acceptable risk or risk appetite. • Identified risks from all levels are reviewed holistically for likelihood and impact to the achievement of agency objectives. • Ensure that as the internal and external environment changes, adjustments are adapted timely.
8. The agency considers the potential for fraud in assessing risks to the achievement of objectives.	• Process in place to identify possible fraud that may occur in the agency's business process. • Fraud risks consider drivers/causes of fraud (incentives, opportunity, and pressures) • Policies and procedures in place so employees are informed and engaged pertaining to job duties, documentation requirements, reviews and approvals, routine meetings, etc. • Establish adequate resources to ensure segregation of duties. • Mandatory ethics training. • Established procedures to report discrepancies or questionable methods/results so they are investigated and appropriate action is determined.	• Agency risk assessment process includes fraud risks in the risk identification process. • Formal fraud risk assessment in addition to annual risk assessment. • Review of control activities to aid in prevention/detection of fraud. • Policies and procedures are written, reviewed, distributed, and compliance is expected. • Cross training and review of responsibilities would ensure employees have sufficient knowledge base to be engaged with the entire process. • All employees are required to attend annual ethics training. • Whistleblower policy is implemented, reviewed, and documented. This is an established, well publicized, and easy to report procedure.

PRINCIPLE	PRESENT	FUNCTIONING
9. The agency identifies and assesses change that could significantly impact the system of internal control.	• Agency monitors for changes in legislation and regulations. • Agency analyzes effects of organization structure changes of personnel and departments. • Agency has a change management model in place to ensure employees are kept current on work related matters as business models/processes change. • Environmental scan included in the strategic planning process.	• Agency counsel monitors proposed/enacted legislation and provides summary of effects on agency operations. • Internal Control Officer, as well as senior leadership is kept updated as to changing environments. • Agency-wide platform to disseminate information, such as emails, website postings and meetings. • Organization structure is documented, available and updated as needed.
10. The agency selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	• Procedures are in place for employees to maintain accurate records of all business transactions (both financial and operational) to ensure completeness and validity. • Procedures implemented to establish a chain of command for entering, authorizing, approving, and reconciling of transactions (segregation of duties). • Access security controls are physical and software processes to prevent or detect unauthorized access to systems and data.	• Employees are aware of procedures through distribution of guidelines and receive training for updated best practices and procedural changes, as necessary. • Departments are required to conduct physical inventories to verify purchase orders as well as use of inventory software for reconciliation purposes. • Use of external auditor to verify and validate purchases and ensure accuracy of recorded transactions. • Unique usernames and passwords are required to gain access to assets, computers, and networks.
11. The agency selects and develops general control activities over technology to support the achievement of objectives.	• Agency has a comprehensive IT network to ensure communication and sharing of information between internal and external departments in the promotion of the efficient execution of agency objectives. • Security measures are established and maintained to prevent compromising technology infrastructure, protection of confidential materials, and data loss (i.e. password protection, firewall, etc.). • Users are granted access to only the system functions needed based on their role with the agency and internal control responsibilities assigned. • User access is reviewed periodically for appropriateness and continued relevance.	• All employees are trained on IT systems and informed of IT policies that affect security of the agency's IT network. • Periodic tests of potential breaches in IT security systems. • Generated reports of findings of attempted breaches and vulnerabilities of the IT system as well as alerts generated for internal, improper use. • Process in place for provisioning and deprovisioning of access requested by users. • Access reviews and certifications performed annually.

PRINCIPLE	PRESENT	FUNCTIONING
12. The agency deploys control activities through policies that establish what is expected and procedures that put policies into action.	• Management establishes policies that clearly outline employee responsibilities, accountability, and support the directives of management in achieving the agency's day-to-day objectives while also mitigating risks. • Policies are formal documents that are available to all staff. • Responsible personnel competently execute policies and procedures in a timely manner to address issues as they arise and to implement corrective action.	• Procedures are in alignment with agency policies, documented, up-to-date, and available to applicable staff. • Obtain periodic confirmations from employees confirming that policies and/or procedures have been received and understood. • Management periodically assesses control activities for continued relevance. • Management conducts and reviews employee evaluations to ensure responsibilities and accountability continues to be performed and met in a timely manner.
13. The agency obtains or generates and uses relevant, quality information to support the functioning of internal control.	• Staff are provided a unique e-mail address to send/receive necessary and required information. • Time keeping systems are used to track time and billable time codes of employees. • Information from internal system reports or external system reports are available to staff. • Hotline(s) is available to employees, customers, vendors, and the public to report improper use information.	• Staff have access to e-mail system(s) and receive necessary and required information directly and timely. • Time keeping systems accurately track hours required to be worked, hours worked, leave accrued/taken and balances per individual for agency staff. Systems are checked and reviewed to ensure information is accurate and approved. • Internal reports are generated timely at required intervals, information is accurate and in a format staff can use/read, system checks/security is accurate to ensure information is correct and safeguarded. • External reports are received and available when needed or required. Information is verified, correct and in a usable format. • Hotline information is available to all staff, external customers and public. Information received from hotline is reviewed and acted upon in a timely fashion.

| PRINCIPLE	PRESENT	FUNCTIONING
14. The agency internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	• Training and education is provided to all agency staff. • Agency website/dashboard for internal control is available to all staff. • Staff demonstrates knowledge of internal controls related to their functions. • Agency commissioner issues clear and concise statement supporting good internal controls process. • Agency has written policies and procedures which are available and known to staff. • Organizational changes are communicated to staff. • Designation of Internal Control Officer and Internal Auditor is known to staff. • Responsibility and timeframes for corrective action plans from internal control program. • Agency commissioner/agency leadership facilitate dialog periodically with all staff through town halls, direct communication, email communication, memorandums, and website postings.	• Agency has scheduled training which all staff is required to attend. • Written and on-line training material is relevant, up to date and available to staff. • Website/dashboard information is accessible, up-to-date and relevant to all staff. • Staff document testing of control activities, identify potential risks and develop control activities to mitigate occurrence. • Agency commissioner issues memo identifying support for a good internal control program, holds periodic town hall meetings with agency, conducts one on one sessions with agency units. • Written policies and procedures are communicated to all staff, updated when necessary and relevant to the functions of the agency. • Agency staff are notified timely of organizational changes through written communications or management/staff meetings • Staff are informed of who within the agency has been designated as the Internal Control Officer and Internal Auditor as well as informed of their purpose within the agency through announcement by Executive staff.
15. The agency communicates with external parties regarding matters affecting the functioning of internal control.	• External audits are conducted by control agencies (i.e. Office of State Comptroller, Federal Single Audit, NYS Financial Statements Audit, etc.). • The Public Information Office/Officer responds to external communication requests on behalf of the agency. • The agency's public website(s) communicates relevant and timely information to external parties (i.e. stakeholders, customers, consumers, vendors, regulators). • A process is in place to accept and respond to correspondence received from external parties. • A process is in place to accept and respond to FOIL requests received.	• Audit reports are received, reviewed, responded to and corrective actions are completed. • A Public Information Office and Officer are designated to handle the "face" of the agency and respond timely to inquiries. • Agency maintains an up-to-date, accurate website which is accessible to the public for disseminate necessary information. • Correspondence with external parties is handled timely and accurately by appropriate staff. • FOIL requests are tracked and responded to timely and thoroughly.

PRINCIPLE	PRESENT	FUNCTIONING
16. The agency selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Ongoing evaluations: • Regularly scheduled staff meetings. • Periodic reconciliations. • Routine reviews of key controls (i.e. monthly, quarterly, semi-annually, annually, or as deemed necessary). • Routine monitoring of large or atypical payment transactions. • Use of dashboards. • Use of aging reports. • Automated software controls to identify unusual transactions. • Regularly scheduled performance evaluations. • Annual agency-wide internal control review. • Routine monitoring occurs of the procurement function for unusual delays in processing and awarding contracts and responds to or communicates the status to the proper individuals in a timely manner.	Ongoing evaluations: • Staff meeting schedule, agenda, or meeting minutes. • Exception reports resulting from periodic reconciliations, aging reports, routine reviews, software control findings. • Documentation demonstrating the use of these ongoing evaluations. • Significant findings and variances are routinely documented and discussed at weekly staff meetings. • Documentation of corrective action taken when exceptions are identified.

	Separate evaluations:
	• Internal Audit evaluations.
	• Other objective evaluations.
	• Benchmarking studies.
	• Peer evaluations.
	• Self-assessments (separate from those conducted in the internal control review program).
	• Outsourced Service Providers (OSPs).
	• Review of compliance with New York Minority and Women-Owned Business Enterprises laws and regulations.
	• Review of payroll and personnel policies and procedures for compliance with NYS laws, rules, regulations, and directives.
		Separate evaluations:
		• Documentation demonstrating the performance of these separate evaluations.
		• Agency responds in writing to external evaluations.
		• Documentation of corrective action taken when exceptions are identified.
		• Report of external evaluations may include information such as:
		   o scope of evaluation,
		   o last evaluation date,
		   o firm name/contact information, and
		   o findings and observations.

PRINCIPLE	PRESENT	FUNCTIONING
17. The agency evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the Board of Directors, as appropriate.	• Internal Control Officer communicates deficiencies identified through the internal control review program to management as applicable. • Internal Audit Department issues audit reports to auditee management, the agency commissioner, and audit committee directly. • Reports from control agencies are issued to the agency commissioner. • A process exists for agency leadership to review observations and recommendations for corrective action by external firm evaluations. (i.e. a cross-functional committee exists to review external evaluation reports and propose corrective actions to agency leadership.) • A process exists for agency leadership to discuss the results of annual risk assessments with the internal controls advisory committee and provide feedback to make corrective actions. (i.e. agency leadership might propose two courses of action to address a negative finding during testing.) • A process exists for regional directors to routinely meet to review the unit's performance and to address improvements.	• Corrective action plans are formally documented. • Status of corrective action plans is tracked by a member of management with sufficient authority to effect change. • Follow-up evaluations are conducted to confirm implementation status. • Agreed upon significant recommendations and corrective actions scheduled and completed are documented. • External evaluation reports with agency responses are communicated to the agency commissioner, and/or Board of Directors. • Agency leadership meets semi-annually with the internal controls advisory committee to communicate or provide updates to short and long term strategic initiatives and goals. The purpose is to inform and assist the committee to focus resources for testing of controls. Results of risk assessments are discussed with each department's management and posted on the internal resource website within a month after completion. • Identified control deficiencies that that may hinder achievement of objectives are documented and action plans are developed and implemented in a timely manner.

OPERATING TOGETHER

The COSO Framework requires that all components operate together in an integrated manner. Operating together refers to the determination that <u>all five</u> components collectively reduce, to an acceptable level, the risk of not achieving an objective.

Management can demonstrate that components operate together when all relevant principles are present and functioning and internal control deficiencies aggregated across components do not result in the determination that one of more material deficiencies exist.
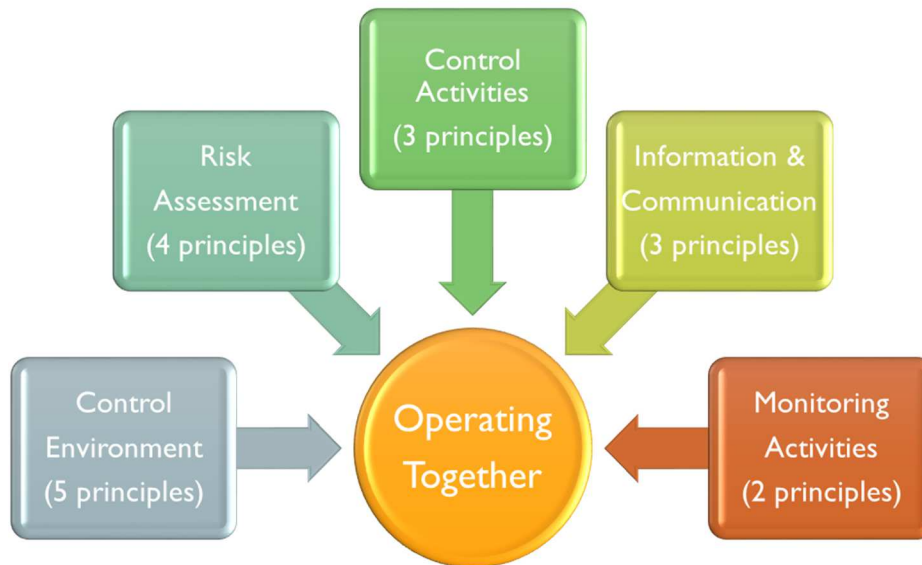
DEFICIENCIES

Management evaluates the significance of identified deficiencies or group of deficiencies. Significance refers to the relative importance of a deficiency to the agency achieving a defined objective. To evaluate the significance of the deficiency, management assesses its effect on achieving the defined objectives at both the agency and transaction level. Management evaluates the significance of a deficiency by considering the nature of the deficiency, the magnitude of impact, and the likelihood of occurrence. The nature of the deficiency involves factors such as the degree of subjectivity involved with the deficiency and whether the deficiency arises from fraud or misconduct. Magnitude of impact refers to the likely effect that the deficiency could have on the agency achieving its objectives and is affected by factors such as the size, pace, and duration of the deficiency's impact. A deficiency may be more significant to one objective than another. Likelihood of occurrence refers to the possibility of a deficiency impacting an agency's ability to achieve its objectives.

INTERNAL CONTROL DEFICIENCY

Internal control deficiency refers to a shortcoming in a component or relevant principle(s) that reduces the likelihood of the agency achieving its objectives. An internal control deficiency in <u>design</u> can arise when a control necessary to meet a control objective is missing or an existing control is not properly designed so that even if the control operates as designed, the control objective would not be met. A control cannot be effectively implemented if it was not effectively designed. An internal control deficiency in <u>implementation</u> exists when a properly designed control is not implemented correctly in the internal control system. A control cannot be effectively operating if it was not effectively designed and implemented. A deficiency in <u>conduct</u> exists when a properly designed control does not operate as designed, or when the person performing the control does not possess the necessary authority or competence to perform the control effectively.

MAJOR DEFICIENCY

Major deficiency refers to an internal control deficiency, or combination of deficiencies, that severely reduces the likelihood that the agency can achieve its objectives. A major deficiency exists in the system of internal control when management determines that a component and one or more relevant principles are not preset or functioning, or that components are not operating together. A major deficiency in one component or principle cannot be mitigated to an acceptable level by the presence and functioning of another component or principle. Deficiencies are evaluated both on an individual basis and in the aggregate. Management considers the correlation among different deficiencies or groups of deficiencies when evaluating their significance. When a major deficiency exists, the agency cannot conclude that it has met the requirements for an effective system of internal control.

DOCUMENTATION

Documentation is required for the effective design, implementation, and operating effectiveness of the internal control system. The level of documentation required will vary, based on the size and complexity of the agency. Management uses judgment in determining the extent of documentation needed, and should be done with cost-effectiveness in mind. Agencies that are subject to audit by the NYS Office of the State Comptroller should be able to produce persuasive evidence that proves controls are designed, implemented, and deployed to effect the components and related principles. The persuasive evidence should be kept in accordance with NYS archives directives and made available upon audit.

Agencies may use, revise and tailor the Component and Principle Evaluation template as they deem fit to document the determination of whether each component and relevant principle is present and functioning, as well as whether all five components are operating together in an integrated manner. The template includes an evaluation summary worksheet and principle evaluation worksheet for each of the 17 principles. This attachment is not required, nor should it be submitted with the annual internal control certification, but should be made available along with supporting documentation upon audit. If your agency elects to use this template, below is an explanation of each section.

COMPONENT AND PRINCIPLE EVALUATION TEMPLATE

EVALUATION SUMMARY WORKSHEET

Each set of principles is color coded by component. Once a determination has been made for a set of principles in a component, return to the evaluation summary worksheet to document your determination of whether the component is present and functioning. For a component to be present and functioning, internal control deficiencies identified for individual principles cannot aggregate to a major deficiency.

Once a determination of present and functioning has been made for each component (see Present and Functioning section for more information), the agency can make a determination of whether all components are operating together in an integrated manner (see Operating Together section for more information). To determine if the overall system of internal control is effective, all components must be present and functioning, and operating together in an integrated manner (see Requirements for Effective Internal Control for more information).

PRINCIPLE EVALUATION WORKSHEET

PRINCIPLE AND POINTS OF FOCUS

The related points of focus are provided on each principle worksheet to help clarify what each principle means. Evaluation for each point of focus is not required (see Suitability and Relevance of Components and Principles section for more information).

EXAMPLES

These are illustrative examples of potential controls your agency may employ to effect the specified principle. Examples are more specific to state government and its operations. This is not meant to be an exhaustive list, nor are all the examples mandatory for compliance. Note that having all the examples listed here in place still does not guarantee passage of an audit by a control agency.

SUMMARY OF CONTROLS TO EFFECT PRINCIPLE

This section is used to document what controls your agency employs in its internal control system. Each of these controls are used in the determination of present and functioning.

PRINCIPLE EVALUATION

Present

Make a determination as to whether the principle exists in the design and implementation of the system of internal controls to achieve specified objectives (see Present section for more information). Space has been provided to detail any internal control deficiencies that have been identified (see Internal Control Deficiency section for more information). If a major deficiency has been identified, provide a brief explanation of the deficiency in last section of the evaluation worksheet. Note that if a major deficiency has been identified, the principle cannot be determined to be present (see Major Deficiency section for more information).

Functioning

For each principle, make a determination as to whether the principle exists in the conduct of the system of internal controls to achieve specified objectives (see Functioning section for more information). Space has been provided to detail any internal control deficiencies that have been identified (see Internal Control Deficiency section for more information). If a major deficiency has been identified, provide a brief explanation of the deficiency in last section of the evaluation worksheet. Note that if a major deficiency has been identified, the principle cannot be determined to be functioning (see Major Deficiency section for more information).

MAJOR DEFICIENCY IDENTIFIED

When a major deficiency exists, the agency cannot conclude that it has met the requirements for an effective system of internal control. A major deficiency exists in the system of internal control when management determines that a component and one or more relevant principles are not preset or functioning, or that components are not operating together. Note that internal control deficiencies may exist, but not aggregate to a major deficiency (see Major Deficiency section for more information).