NEW YORK STATE
ENERGY RESEARCH AND DEVELOPMENT AUTHORITY

# INTERNAL CONTROL MANUAL:
# Ensuring Efficiency, Accountability, and Transparency

Revised January 2018

TABLE OF CONTENTS

## SECTION 1: PURPOSE; BOARD MEMBER RESPONSIBILITIES

The purpose of this manual is to set forth NYSERDA's policies and procedures for ensuring an effective system of internal controls that also promotes accountability and transparency.

Public Authorities Law, Article 9, Title 8, §2931, known as the New York State Governmental Accountability Audit and Internal Control Act ("Internal Control Act") requires NYSERDA to establish and maintain a system of internal controls. The Internal Control Act defines internal controls as a "process that integrates the activities, plans, attitudes, policies, systems, resources and efforts of the people of an organization working together, and that is designed to provide reasonable assurance that the organization will achieve its objectives and mission" (Article 9, §2930).

The Internal Control Act lists specific objectives of an internal control system including, but not limited to:

- the safeguarding of assets;
- checking the accuracy and reliability of accounting data and financial reporting;
- promoting the effectiveness and efficiency of operations;
- ensuring compliance with applicable laws and regulations; and
- encouraging adherence to prescribed managerial policies.

The Public Authorities Accountability Act of 2005, which amends various sections of the Public Authorities Law, seeks to ensure greater efficiency, openness and accountability for the State's public authorities by codifying model governance principles, removing legal impediments that prevent full implementation of model governance principles, establish a new public authorities office within the Executive Department to provide additional oversight and ensure full compliance with the principles, and allow for the creation of an independent inspector general to ensure greater accountability for public authority activities and operations.

As explained below and through their review and approval of various guidelines, reports, planning documents, and other activities of NYSERDA staff, NYSERDA's Board Members are actively engaged in overseeing NYSERDA use of processes, policies, and procedures that accomplish NYSERDA's mission through an effective system of internal controls that incorporates accountability and transparency.

**Board Member Internal Control Responsibilities.** The Internal Control Act requires that the governing board of NYSERDA:

- establish and maintain for NYSERDA guidelines for a system of internal control that are in accordance with this article and internal control standards;
- establish and maintain for NYSERDA a system of internal control and a program of internal control review. The program of internal control review shall be designed to identify internal control weaknesses, identify actions that are needed to correct actions and periodically assess the adequacy of NYSERDA's ongoing internal controls;
- make available to each Board Member, officer and employee a clear and concise statement of the generally applicable managerial policies and standards with which he or she is expected to comply. Such statement shall emphasize the importance of effective internal control to NYSERDA and the responsibility of each Board Members, officer and employee for effective internal control;
- designate an internal control officer, who shall report to the head of NYSERDA, to implement

and review the internal control responsibilities established pursuant to this section;
- implement education and training efforts to ensure that Board Members, officers and employees have achieved adequate awareness and understanding of internal control standards and, as appropriate, evaluation techniques; and
- periodically evaluate the need for an internal audit function.

**Board Member Accountability Responsibilities.** The Public Authority Accountability Act of 2005 requires the Board Members to:

- execute direct oversight of NYSERDA's President and CEO and other senior management in the effective and ethical management of NYSERDA;
- understand, review and monitor the implementation of fundamental financial and management controls and operational decisions of NYSERDA;
- establish policies regarding the payment of salary, compensation and reimbursements to, and establish rules for the time and attendance of the President and CEO and senior management;
- adopt a code of ethics applicable to each officer, director and employee that, at a minimum, includes the standards established in section seventy-four of the public officers law;
- establish written policies and procedures on personnel including acts of wrongdoing, misconduct, malfeasance, or other inappropriate behavior by an employee or Board Member of NYSERDA, investments, travel, the acquisition of real property and the disposition of real and personal property and the procurement of goods and services;
- adopt a defense and indemnification policy and disclose such plan to any and all prospective Board Members; and
- attend State approved training, including such continuing training as may be required to remain informed of best practices, regulatory and statutory changes relating to the effective oversight of the management and financial activities of public authorities and to adhere to the highest standards of responsible government.

Through all of the processes, policies, and procedures set forth in this manual, the three underlying manuals (the Personnel Handbook, Information Security Policies Manual, Accounting Policies and Procedures Manual, and Operations and Procedures Manual), and through its review and approval of a diverse set of guidelines, reports, planning documents and more detailed Committee review of staff activities, NYSERDA's Board Members comply with these statutory requirements.

NYSERDA's Board has established the following standing committees:

Audit and Finance Committee. The Audit and Finance Committee is a standing advisory committee of the Authority. The Committee has not fewer than three or more than six Board Members. The Committee shall consist of not less than three independent Board Members who shall constitute a majority on the Committee and who shall possess the necessary skills to understand the duties and function of the Committee, provided, however, that in the event that there are less than three independent Members, the Members may appoint non-independent Members, provided that the independent Members constitute a majority of the Members of the Committee. In addition, the membership of the Committee includes the Chair of the Authority who serves ex-officio and who enjoys all the rights and privileges of membership, including the right to vote. A majority of the members of the Committee then in office, not including the Chair of the Authority, gathered together in the presence of each other or through the use of videoconferencing, constitutes a quorum, and the Chair of the Authority if present counts toward a quorum. Members of the Committee shall

be familiar with corporate financial and accounting practices.

The Audit and Finance Committee recommends the hiring of a certified independent accounting firm, establishes the compensation to be paid, and provides direct oversight of the performance of the independent audit performed, reviews the annual financial statements of the Authority prior to submission for approval to the Board Members of the Authority, reviews proposals for the issuance of debt by the Authority and makes recommendations, and may examine and consider such other matters in relation to the internal and external audit of the Authority's accounts, the Authority's financings, and in relation to the financial affairs of the Authority and its accounts as the Audit and Finance Committee may determine to be desirable.

Program Planning Committee. The Program Planning Committee is a standing advisory committee of the Authority. The Committee has not fewer than three or more than six Board Members, who are elected from among the Board Members of the Authority other than the Chair. A majority of these committee members are other than Board Members of the Authority who serve ex-officio. In addition, the membership of the Committee includes the Chair of the Authority, who serves ex-officio and who enjoys all the rights and privileges of membership, including the right to vote. A majority of the members of the Committee then in office, not including the Chair, gathered together in the presence of each other or through the use of videoconferencing, constitutes a quorum, and the Chair of the Authority if present counts toward a quorum.

The Program Planning Committee reviews the annual updating of the Authority's Strategic Program Plan; and preparation of the portions of the Authority's annual budget related to the energy research and innovation, market development, clean energy financing, and other related programs and initiatives; and provides guidance to the Authority's officers and employees in the preparation of those plans and those portions of the budget; and considers such other matters related to the Authority's energy research and development programs, energy services programs, energy analysis program, and economic development program as the officers of the Authority may refer to the Committee.

Waste and Facilities Management Committee. The Waste and Facilities Management Committee is a standing advisory committee of the Authority. The Committee has not fewer than three or more than six members, who are elected from among the Board Members of the Authority other than the Chair. A majority of these committee members are other than Board Members of the Authority who serve ex-officio. In addition, the membership of the Committee includes the Chair of the Authority, who serves ex-officio and who enjoys all the rights and privileges of membership, including the right to vote. A majority of the members of the Committee then in office, not including the Chair of the Authority, gathered together in the presence of each other or through the use of videoconferencing, constitutes a quorum, and the Chair of the Authority if present counts toward a quorum.

The Waste and Facilities Management Committee reviews the Authority's program and plans for management of the Western New York Nuclear Service Center, including the West Valley Demonstration Project, and for radioactive waste policy and nuclear coordination; reviews the preparation of the Authority's annual West Valley site management program and radioactive waste policy and nuclear coordination budgets; provides guidance to the Authority's officers and employees in the preparation of the plans and in preparation of such annual program budgets; and considers such other matters related to West Valley site management and radioactive waste policy and

nuclear coordination programs as the Officers of the Authority may refer to such Committee.

Governance Committee. The Governance Committee is a standing advisory committee of the Authority. The Committee shall consist of not less than three independent Members who shall constitute a majority on the Committee and who shall possess the necessary skills to understand the duties and function of the Committee, provided, however, that in the event that there are less than three independent Members, the Members may appoint non-independent Members, provided that the independent Members constitute a majority of the Members of the Committee. The Committee has not fewer than three or more than six members. In addition, the membership of the Committee includes the Chair of the Authority who shall serve ex-officio and who enjoys all the rights and privileges of membership, including the right to vote. A majority of the members of the Committee then in office, not including the Chair of the Authority, gathered together in the presence of each other or through the use of videoconferencing, constitutes a quorum, and the Chair of the Authority if present counts toward a quorum.

The Governance Committee keeps the Board Members informed of current best practices, reviews corporate governance trends, updates the Authority's corporate governance principles, as necessary, recommend updates to the corporate governance principles, advises appointing authorities on the skills and experience required of Board Members, examine ethical and conflict of interest issues, perform Board self-evaluation, and recommend By-laws which include rules and procedures for conduct of Board business.

All meetings of the Authority subject to the Open Meetings Law will be broadcast on the Internet.

**Board Member Compliance with Lobbying Laws**

Procurement Lobbying: State Finance Law Sections 139-j and 139-k applies to all solicitations issued and procurements under active consideration that may result in a procurement contract in an amount in excess of $15,000. Such solicitations and procurements under consideration must: (1) designate individuals at NYSERDA who may be contacted about the procurement by persons attempting to influence the procurement process (*i.e.,* offerers and persons hired by the offerer who attempt to influence the procurement), and (2) outline NYSERDA's procedures relating to contacts that are not permitted under the State Finance Law. All solicitations and procurements will identify NYSERDA employees, and not Board Members, as the individuals that may be contacted under such circumstances.

The responsibility to record information about contacts that reasonably appear to be attempts to influence the procurement process applies during the "restricted period." The restricted period begins once NYSERDA has made a decision to initiate procurement and extends until execution of the contract. It begins again at any time a modification to the contract is proposed and extends until the modification is executed.

The decision to initiate procurement occurs at the earliest of: (1) the Greenlight Committee's approval of the proposed issuance of a solicitation, (2) an employee's receipt of a proposal for a program project that does not meet the definition of Competitive Procurement Method under the Contracting Guidelines, or (3) at such other time when a determination is made to proceed with an administrative procurement. At this time and until the time a contract is executed, Board Members must: (1) record information regarding contacts that reasonably appear to be attempts to

influence the procurement process within the restricted period, and (2) submit the record to

NYSERDA's Director of Contract Management who will maintain such records in the appropriate file. The record is to include the contact including the name, the organization, the address, the telephone number, the place of principal employment, and the occupation of the contact and whether the person or organization making the contact is a "potential contractor" or is retained, employed, or designated by the potential contractor to appear before or to contact the agency regarding the procurement.

Failure to comply with the requirements may result in a contractor being barred from governmental procurements. Board Members should contact the General Counsel if they have any questions concerning these requirements.

Project Sunlight: Project Sunlight, a component of the Public Integrity Reform Act of 2011, is intended to provide the public with an opportunity to see when outside individuals and entities are interacting with—and attempting to influence—state government decision-makers in particular ways. Project Sunlight requires the reporting in an online database of all interactions that constitute "appearances" between "covered individuals" inside NYSERDA and "covered individuals" outside NYSERDA concerning one of five designated Project Sunlight subject areas.

An "appearance" is an in-person meeting, telephonic conversation, or video conference that is a substantive interaction meant to influence state government decision-making. The location, formality, and initiator of the interaction are irrelevant. Excluded from "appearance" are all written communications; administrative or ministerial interactions; purely informational exchanges; interactions regarding legislation or the budget; and meetings that are open to the public. NYSERDA "covered individuals" are those individuals designated as "policy-makers," which includes Board Members. "Covered individuals" outside NYSERDA include internal and external representatives of outside entities, individuals representing themselves, and representatives of advocacy groups. Not included are employees of other state agencies and of other governments; state elected officials, executive and legislative employees, judges, and employees of the judiciary; representatives of the media; and persons under the age of 18. An "appearance" between "covered individuals" must be reported if it concerns one of five designated subject areas: procurement (outside of the restricted period defined by the Procurement Lobbying Law), regulatory matters, rule making, judicial or quasi-judicial proceedings, and rate making.

Reportable appearances must be timely recorded in the database, within five business days after they occur. NYSERDA covered individuals complete the Project Sunlight reporting form available on NYSERDA's intranet and emails it to the dedicated email inbox: projectsunlight@nyserda.ny.gov. NYSERDA's Project Sunlight Liaison, designated by the General Counsel, coordinates and oversees NYSERDA's reporting efforts. Board Members should contact the Project Sunlight Liaison or General Counsel if they have any questions concerning these requirements.

Regulatory Lobbying: Public Authorities Law §2987 requires every Member, Officer, or employee to record all contacts, whether oral or written, that are an attempt to influence the adoption or rejection of any rule or regulation having the force and effect of law that is issued by NYSERDA. The record must include the day and time of the contact, the identity of the lobbyist, and a general summary of the substance of the contact. NYSERDA shall maintain these records for not less than seven years.

**INTERNAL CONTROL POLICY**

It is the responsibility of every employee to abide by the requirements of the internal controls system. All employees are expected to be aware of NYSERDA's internal controls system and regularly consider the system in performing their tasks. NYSERDA has prepared a Code of Conduct, attached hereto as Appendix B, summarizing a number of basic standards and State and Federal laws which NYSERDA employees are required to follow. The Code of Conduct sets forth NYSERDA's expectations that its employees conduct themselves in an honest and ethical manner and is provided to all employees.

If an employee identifies a potential weakness in, or deviation from, NYSERDA's internal control systems or generally accepted systems of internal controls, he or she shall report such potential weakness or deviation immediately in accordance with NYSERDA's Whistleblower Policy, attached hereto as Appendix C.

## INTERNAL CONTROL SYSTEM

The procedures herein establish checks and balances over NYSERDA's administration and operations practices, financial and accounting practices and personnel practices, regularly reviewing the adequacy of the controls, especially in areas of highest vulnerability, revising those controls as necessary to reflect organizational changes, new program mandates or staffing adjustments, and taking corrective action when internal control weaknesses are identified. NYSERDA stresses to its Directors and they to their staffs the importance of communicating and adhering to the policies and procedures in the Internal Control System.

The Internal Control Officer is responsible for assisting with the implementation and review of the internal control system and for implementing education and training of staff.

All employees and officers have access to all the manuals that comprise the internal control system which are:

- Internal Control Manual – the compilation of the accounting, operating and administrative controls of NYSERDA as described more fully in the following manuals:

- Operations and Procedures Manual – details the policies and procedures followed in planning and implementing NYSERDA's programs and administration, including its contracting process to ensure compliance with State statutes, regulatory requirements and Executive Orders;

- Accounting Policies and Procedures Manual – details the financing and accounting practices; and

- Personnel Handbook – details NYSERDA's personnel practices and policies which apply to all employees.

This manual also summarizes the primary functions and control objectives of each of NYSERDA's assessable units. Assessable units are defined in the Comptroller's Internal Control Standards, as units which perform a distinct function or service and/or that fulfill a law, regulation or mandate. NYSERDA's assessable units include:

- Energy Programs (Market Development, Innovation and Research, and other energy program activities)
- NY Green Bank
- Policy & Regulatory Affairs

- Radioactive Waste Management
- Bond Financing
- Contracts Management
- Accounting
- Human Resources
- Computer Systems
- Counsel's Office
- Governmental Affairs
- Communications
- Corporate Marketing
- Consumer Services and Events Management
- Internal Audit

All staff shall maintain NYSERDA records in accordance with the General Retention and Disposition Schedule for New York State Government Records.

**INTERNAL CONTROL TRAINING AND AWARENESS**

The Internal Control Officer shall coordinate training and awareness activities to ensure that all NYSERDA employees have an understanding of internal control principles and how they relate to the performance of their work assignments.

In addition, the Internal Control Officer and executive management shall periodically communicate to NYSERDA staff regarding internal control principles and responsibilities, not less frequently than once each year.

## INTERNAL CONTROL REVIEW PROCESS

The Internal Control Officer shall coordinate a process of organization-wide risk assessment not less frequently than once every three years. The risk assessment shall identify significant risks which threaten the achievement of unit/organizational objectives, the controls in place to eliminate or mitigate these risks, and an assessment of the relative likelihood of occurrence and the impact of such risks (using a rating system to be established by executive management). Each risk assessment shall be reviewed and approved by the manager's supervisory personnel through executive management, and shall also be provided to the Director of Internal Audit for review and comment. The results of the organization wide risk assessment shall be communicated to the Audit and Finance Committee for review and comment.

In addition, the Internal Control Officer shall convene a multi-disciplinary internal control working group not less frequently than once a year to review NYSERDA's internal control policies and procedures, organizational structure and inventory of functions, and to consider and recommend changes to improve internal controls.

The Internal Control Officer shall be responsible for monitoring the implementation of corrective actions which result from internal control reviews, internal control testing, internal audit reports, or reports issued by external auditors related to internal control matters. The Internal Control Officer shall provide a report to the President and CEO not less frequently than annually summarizing the status of all such corrective actions.

**INTERNAL CONTROL TESTING**

To supplement the ongoing evaluation of the adequacy of NYSERDA's internal controls, NYSERDA shall conduct periodic compliance testing, at least annually, to determine the extent to which staff follow prescribed policies and procedures.

## ANNUAL REPORTING

NYSERDA prepares the annual report required by Section 2800 of the Public Authorities Law and submits it to the Board Members for review and approval. The report is certified in writing by the President and CEO and the Treasurer that based on his or her knowledge the information provided therein is accurate, correct and does not contain any untrue statement of material fact, does not omit any material fact which, if omitted, would cause the financial statements to be misleading in light of the circumstances under which such statement are made and fairly presents in all material respects the financial condition and results of operations of NYSERDA as of and for the periods presented in the report.

Attached as part of the annual report is a copy of the annual independent audit report, performed by a certified public accounting firm in accordance with generally accepted government auditing standards, and management letter with any other external examination of the books and accounts (other than reports of any examinations made by the State Comptroller).

This annual report is submitted to the persons designated by Sections 2800 and 2802 of the Public Authorities Law.

NYSERDA also submits the annual internal control certification and report in accordance with requirements established by the Authorities Budget Office.

## SECTION 2: ENERGY PROGRAMS

## (MARKET DEVELOPMENT, INNOVATION AND RESEARCH, AND OTHER ENERGY PROGRAM ACTIVITIES)

### Primary Functions

- Program Planning Program Development
- Project Development
- Project Management Metrics Reporting

### Controls

Program Planning

NYSERDA's multi-year strategic plan (Plan) includes goals, objectives, and funding for each program. Staff presents the Plan to NYSERDA's Program Planning Committee annually for review and approval. The Program Planning Committee is composed of NYSERDA Board members and is charged with reviewing, amending, and recommending approval of the Plan to the members of the Board. NYSERDA's Board must approve the Plan before it can be implemented by NYSERDA.

Program Development

Programs must operate in manner that is consistent with the Plan as approved by NYSERDA's Board. Programs must operate in a manner that is also consistent with any approved operating plan, funding agreement, Public Service Commission Order, law or regulation related to the program funding source. The Team Lead of each program is primarily responsible for development and implementation of their program area, for consistency with the Board-approved Plan, and for ensuring the collection and tracking of all required information and metrics needed for compliance filings according to the Public Authorities Law and other statutory and administrative requirements, in consultation with oversight provided by the Officer or Business Unit Lead (an employee that reports to the President with oversight of a Program or administrative area that has one or more Team Leads reporting to them) responsible for such Team.

Project Development

NYSERDA uses its best efforts to use competitive methods for selecting contractors, pursuant to Article III: Requirements regarding selection of contractors of NYSERDA's Contracting Guidelines, as adopted by the Board. In addition, projects selected for funding must be consistent with the goals and objectives of the Plan. Solicitations are developed by a Project Manager working in conjunction with a multi-disciplinary team (Team) comprised of: the Team Lead, an assigned attorney from Counsel's Office, and an assigned contract administrator from the Contracts Management department. Once approved by the Team, the request is approved by the Business Unit Lead[1]. Solicitation results are reviewed by a Scoring Committee based upon the evaluation criteria set forth in the Solicitation document. The results of the Scoring

[1] Business Unit Leads are defined as any employee that reports to the President with oversight of a Program or administrative area that has one or more Team Leads reporting to them. In cases where Team Leads report to the President, the President may serve as Business Unit Lead or designate the authority to another Business Unit Lead.

Committee are summarized by the Project Manager, reviewed by the Team and approved by the Business Unit Lead.

Project Management

The Project Manager is responsible for developing, in conjunction with the contractor, a clear and defined project statement of work (SOW), budget, and implementation schedule. The Project Manager is responsible for monitoring and oversight of the contractor's performance to ensure that it adheres to the work required under the contract while anticipating and resolving technical and administrative problems arising during the project. Project Managers communicate with contractors, review progress reports, conduct site visits, review and approve contractor invoices, review and approve technical reports, and approve final project reports.

Metrics reporting

Programs shall be responsible for collecting all relevant data to measure program progress according to predetermined metrics, such as data that can be used to address the anticipated energy, environmental and economic benefits that are realized by projects, and as required by each operating plan or reporting requirement. All estimates shall reference credible sources and estimating procedures, and all assumptions shall be documented. This data will also be used to evaluate program impacts and progress towards goals.

## SECTION 3: NY GREEN BANK

### Primary Functions

- Business Planning
- Business Operation
- Procurement Activities
- Financial Investments
- Portfolio Management
- Metrics Reporting

### Controls

Business Planning

In addition to participating in NYSERDA's Multi-Year Strategic Program Plan, as described in Section 2, Program Planning, above, NY Green Bank develops an annual Strategic and Business Plan (Business Plan). NY Green Bank staff presents the Business Plan to NY Green Bank's Investment and Risk Committee (IRC) annually for review and approval. The IRC is composed of the President and Chief Executive Officer of NYSERDA, Treasurer of NYSERDA, President of NY Green Bank, and one or more NY Green Bank Managing Directors. The IRC is charged with reviewing and approving the Business Plan. The IRC must approve the Business Plan before it can be implemented by NY Green Bank.

Business Operation

NY Green Bank must operate in a manner that is consistent with the Business Plan, as approved by the IRC. In addition, NY Green Bank must operate in a manner that is consistent with any approved operating plan, funding agreement, Public Service Commission Order, law or regulation related to its funding source(s).

NY Green Bank's President reports to the President and Chief Executive Officer of NYSERDA, and Managing Directors report to the President of NY Green Bank. In its operations, NY Green Bank follows the NY Green Bank Operations and Procedures Manual, which is incorporated by reference into NYSERDA's Operations and Procedures Manual, forms part of NYSERDA's system of internal controls, and is designed to supplement existing NYSERDA controls.

The President of NY Green Bank is primarily responsible for oversight of the operations of NY Green Bank in a manner that is consistent with the Business Plan and the NY Green Bank Operations and Procedures Manual, and for ensuring the collection and tracking of all required information and metrics needed for compliance filings according to the Public Authorities Law and other statutory and administrative requirements.

Procurement Activities

When NY Green Bank procures goods and services, it does so subject to NYSERDA's Contracting Guidelines, as adopted by the Board, and the procedures summarized in Section 2, Project Management, above.

Financial Investments

Potential financial investments that are considered for funding by NY Green Bank must meet the requirements of its investment process, including minimum investment criteria prescribed by the Public Service Commission (the "PSC") and specific evaluation criteria. All such criteria, along with NY Green Bank's investment process, are consistent with NY Green Bank's goals and objectives, and are set out in various PSC Order and public filing made by NY Green Bank. NY Green Bank's origination of clients, counterparties, collaborators, and potential transactions results from interactions with market participants who submit proposals that either: (i) respond to a NY Green Bank- specific solicitation and/or other publication of NY Green Bank's investment criteria (a Competitive Opportunity) or (ii) identify a NY Green Bank role consistent with its mandate, but which does not strictly fall within the definition of "Competitive Opportunity" (Strategic Opportunity).

While open and public competitive processes are favored in the origination of NY Green Bank, clients, counterparties, collaborators and transactions, it is nevertheless recognized that there may be circumstances in which the strategic mission of NY Green Bank is best served by undertaking one or more Strategic Opportunities. Strategic selection methods may be utilized if it is determined by NY Green Bank management, with approval from the IRC, that the opportunity: (i) is presented by a private sector party with exceptional, relevant experience and expertise; (ii) is one-of-a-kind by virtue of location, high visibility, probability of a successful closing or leverage with other already committed private or public funding or possesses other unique attributes; (iii) has exceptionally strong compatibility with the strategic objectives and mandate of NY Green Bank; (iv) represents an urgent need as a result of public exigency or emergency, or would become unavailable as a result of delay, or would take an unacceptable length of time for a similar opportunity to reach the same level of readiness; and/or (v) relates to the next phase of a multiphase proposal or the expenditure is necessary to support or protect an existing NY Green Bank investment or initiative.

Competitive Opportunities are designed to comply with the definition of a "competitive procurement" set forth in the Office of the State Comptroller Rules, Part 206 to NYCRR Title 2 (Comptroller's Regulations). For any proposed Strategic Opportunity involving NY Green Bank funding that will exceed $1 million, NY Green Bank staff consults with NY Green Bank's internal counsel regarding the application of the Comptroller's Regulations.

Prior to issuing a solicitation for a Competitive Opportunity, or to undertake a Strategic Opportunity, NY Green Bank staff develops a summary thereof (Opportunity Summary) for review and approval by the IRC. Once an Opportunity Summary for a Competitive Opportunity is approved by the IRC, NY Green Bank personnel prepares that solicitation in collaboration with NYSERDA's Contract Administrator and Counsel's Office. The solicitation takes into account any comments or qualifications made by the IRC in conjunction with its approval. In the case of an Opportunity Summary for a Strategic Opportunity, once approved by the IRC, NY Green Bank initiates due diligence.

For Competitive Opportunities, a proposal evaluation and scoring committee, consisting of at least three (3) internal members who are designated by the President of NY Green Bank, evaluates proposals for transactions arising from NY Green Bank solicitations and recommends those opportunities that best meet NY Green Bank's published investment criteria. Opportunities recommended by the committee will be subject to more detailed exploration and analysis.

For proposals selected for further exploration, whether as the result of a Competitive or Strategic Opportunity, NY Green Bank staff further evaluates and negotiates the proposed transaction and will prepare a Greenlight Memorandum (except in extraordinary circumstances that may permit a proposal to be immediately submitted to the IRC), which provides an analysis of the transaction. A Greenlight Committee, composed of at least three members of the IRC, reviews those transactions selected by staff for advancement, and may make general recommendations, or recommend required contingencies or conditions with regard to a proposed transaction, may recommend additional due diligence, or may recommend rejection of a proposed transaction. If the Greenlight Committee recommends rejection of a transaction, the recommendation shall be brought to the President and Chief Executive Officer of NYSERDA, who shall decide whether to accept the recommendation, or who may decide to require conditions or contingencies that have to be met in order for the transaction to proceed. When transactions are being considered, members of the Greenlight Committee and IRC will recuse themselves where there are any conflicts of interest.

For transactions receiving a recommendation to proceed in accordance with the above , NY Green Bank staff continues to evaluate and negotiate the proposed transaction. A Transaction Approval Memorandum, which provides a comprehensive analysis of a transaction, is then presented to the IRC for review and approval. E ach IRC member is given the opportunity to submit comments, make recommendations, or suggest contingencies with regard to a proposed transaction, or may recommend additional due diligence. Once each IRC member is given the opportunity to comment and provide recommendations, the President and Chief Executive Officer of NYSERDA may approve or reject the transaction, either of which may require conditions and contingencies.

For approved transactions, assigned staff, along with any retained consultants, will then proceed to finalize any remaining diligence and all transaction documentation, taking into account any recommendations and contingencies expressed by the IRC. Only after transaction approval and only if the agreements are according to all material aspects of the transaction approval may a binding commitment or documentation be executed.

Any proposed post-closing modification to the terms and conditions of a transaction that may cause a material change in the investment outcome will be reviewed by the IRC, in accordance with the procedures set forth above for an original approval.

Portfolio Management

NY Green Bank monitors all of its investments (irrespective of whether funded or unfunded commitments are involved) pursuant to monthly, quarterly and annual transaction reviews to assess performance; quarterly reviews that compare operating and financial results and investment value with expectations; and quarterly portfolio and pipeline reviews with the IRC. NY Green Bank assesses and rates the risk associated with each transaction individually and monitors these risks on an individual and portfolio basis, maintaining overall risk of loss within defined limits.

NY Green Bank also regularly reviews information received in connection with metrics on its investments (both internal and those for disclosure through required periodic public reporting).

The IRC reviews portfolio reports, and will make portfolio-related recommendations, as well as recommendations on the disposition of transaction waivers, amendments, and restructurings as may be required or presented for approval.

Metrics Reporting

NY Green Bank shall be responsible for collecting certain data to support the calculation and reporting of agreed operational, risk management and financial metrics. In addition, NY Green Bank, in collaboration with other Authority staff, shall collect and process certain data required to assess the anticipated energy, environmental and economic benefits, as well as financial market impacts, that are realized by NY Green Bank's investments in clean energy projects, and as required by any applicable PSC Order or reporting requirement. All estimates shall reference credible sources and estimating procedures, and all key assumptions shall be documented. This data will be used to evaluate impacts and progress towards goals.

## SECTION 4: ENERGY AND ENVIRONMENTAL ANALYSIS AND PROGRAM EVALUATION

### Primary Functions

- Modeling and Analytics
- Data and Markets
- Policy Development
- Environmental Research
- Program Evaluation

### Control Objectives

Modeling and Analytics

*Statewide Energy Planning*

Energy and Environmental Analysis provides a coordinating and leadership role on behalf of NYSERDA in the development and preparation of the statutorily-mandated State Energy Plan. Energy and Environmental Analysis oversees the overall State Energy Plan process, including scope development, coordination of participating agencies and authorities, stakeholder outreach, scheduling, deliverables from other agencies, writing, editing, and document and website management.

The President and CEO of NYSERDA serves as the Chair of the Energy Planning Board, which consists of the chief executives from the 15 designated agencies and authorities who have responsibilities that affect or are affected by energy policy. The Director of Energy and Environmental Analysis serves as the Director of the Energy Coordinating Working Group, which functions as the staff arm of the Energy Planning Board. Analyses, documents and all costs associated with the coordination, development and production by Energy Analysis staff to support the State Energy Plan process are reviewed by the Energy Analysis Director and ultimately by the Chair of the Energy Planning Board.

*Modeling and Forecasting*

Energy and Environmental Analysis performs quantitative analyses using a wide range of analytical tools to provide the underpinnings for State policy and program development, regulatory initiatives, and energy decision- making. Responsibility for review, accuracy, and relevance of the various analyses and discussion papers developed is generally held by the Team Lead depending on the nature and sensitivity of the assignment.

Data and Markets

*Energy Data Clearinghouse*

Energy and Environmental Analysis serves as a source for NY State energy-related data and information. This program collects, compiles, maintains, and publishes a wide range of energy data, making extensive use of NYSERDA's web site to reach stakeholders. Information is reviewed by the responsible Team Lead prior to release.

*Energy Markets Monitoring & Intelligence*

Energy and Environmental Analysis monitors New York's major energy supply industries, including petroleum (liquid fuels), natural gas, coal, and electricity. Responsibility for review, accuracy, and relevance of the various analyses and discussion papers developed is generally held by the Team Lead depending on the nature and sensitivity of the assignment.

*State Energy Emergency Planning and Response*

Under Section 5-117 of the Energy Law, NYSERDA is responsible for developing and maintaining the New York State Energy Emergency Plan. Energy and Environmental Analysis maintains a process for annual review and update of the Energy Emergency Plan to assure the Plan is accurate, timely, and can be readily implemented as needed. In addition to Energy and Environmental Analysis, numerous State agencies including the Department of Public Service, Office of Emergency Management, and Office of Homeland Security contribute to the annual review.

*Radioactive Waste Policy and Nuclear Coordination.*

As required by Section 1854-d(1) of Public Authorities Law and Part 502 of Chapter XI of Title 21 NYCRR, Energy and Environmental Analysis collects and maintains data on the generation of low-level radioactive waste by facilities in the State and the subsequent storage, treatment, and disposal of that waste. After review by NYSERDA executive management, an annual final report is provided to the Governor and Legislature NYSERDA is the State's lead agency for addressing radioactive waste policy issues. NYSERDA is the State's lead agency for addressing radioactive waste policy issues. Pursuant to NYSERDA's mandate under Section 7-101 of the Energy Law, Energy and Environmental Analysis coordinates the State's radioactive materials regulatory programs, and the State's oversight of nuclear power plant activities. Staff also provides technical nuclear engineering support to the New York State Department of Health as part of the State's nuclear power plant emergency preparedness and response program. Significant issues, communications and reports are reviewed and approved by senior management as appropriate.

<u>Policy Development</u>

*State Energy Policy Development*

Energy and Environmental Analysis supports, coordinates or leads in the development of specific energy policies, and provides both quantitative and qualitative analysis of policy development and program implementation support. Areas of policy development support work include environmental, fuel and electricity financial and trading markets. Energy and Environmental Analysis provides draft policy initiative documents to Senior Management for approval prior to being distributed outside of NYSERDA.

*NYSERDA Program Development*

Program offerings within NYSERDA are planned and designed in a cooperative manner. Energy and Environmental Analysis participates in this process to help insure that the programs as designed and delivered are likely to achieve or exceed their stated goals and can be properly evaluated. In addition, as evaluation findings and conclusions are completed on specific programs, Energy and Environmental Analysis provides a formal feedback loop to the program implementation teams for improved program design and delivery, as warranted.

*NYSERDA Strategic Planning*

Annually, the Authority develops a Strategic Plan, which describes how the Authority will pursue its mission, goals, and objectives over the ensuing three years, Energy and Environmental Analysis meets with senior management and program staff to discuss and evaluate goals and strategy options, and reviews and researches program planning documents. Energy and Environmental Analysis prepares a draft and a final version of the Plan, which is reviewed by senior management before sending to the Program Planning Committee and the Board for approval.

*Regulatory Affairs and Administrative Proceedings*

Energy and Environmental Analysis actively monitors NYSERDA's interests in regulatory and administrative proceedings related to the State's energy and environmental policy goals, including those of the New York State Public Service Commission and Department of Environmental Conservation rulemakings. Energy and Environmental Analysis staff participates on internal teams with Counsel and other program staff to address particular issues or proceedings, helping to compile and analyze data, and prepare formal submissions, which are approved by senior management prior to submission.

Federal Energy Policy and Planning

Energy and Environmental Analysis maintains relationships with national organizations and stakeholders in the energy arena in order to influence policy and program agendas, to track emerging policy trends and to coordinate NYSERDA responses based on the possible impact on existing or future programs, with senior management approval. In addition, Energy and Environmental Analysis identifies and works with other staff to pursue high value opportunities for collaboration with other state agencies, regional organizations, and neighboring states, with the goal of leveraging our resources and creating a larger impact. Energy and Environmental Analysis in cooperation with other staff also tracks federal solicitations to develop partnerships and high quality responses in areas consistent with NYSERDA's program and policy objectives.

Environmental Research

Energy and Environmental Analysis supports environmental monitoring and associated research and analysis that are critical for assessing and quantifying the environmental soundness and effectiveness of energy programs, and for providing the foundation for researchers and policymakers to design and implement the most effective policies and programs. Energy and Environmental Analysis relies upon a network of professional contacts and working groups of science and policy experts to identify critical gaps and research needs in New York State. Multiple groups, including both the established Program Advisory Group and Science Advisory Committee, provide guidance on the areas representing the major issues and cutting edge scientific understanding related to energy-related environmental impacts. The results of this input are compiled into a comprehensive Research Plan designed to guide energy-related environmental research in New York State. The network of professional contacts also assists in measuring progress of environmental research activities.

Program Evaluation

Performance and Market Standards is responsible for evaluating NYSERDA's market development, innovation and research, and other energy program activities. Performance and Market Standards is structured to assess the effectiveness of programs toward achieving the State's public policy goals. Performance and Market Standards conducts evaluation using competitively selected, expert evaluation contractors who measure and verify impacts attributable to NYSERDA's program activities and examine program efficiency and effectiveness.

NYSERDA reports monthly, quarterly, and annually on the performance of various programs to the Governor, the New York State Legislature, the Public Service Commission, other program sponsors, advisory groups and stakeholders based upon reporting requirements established by the program sponsor. NYSERDA program staff and management are integral to the evaluation process, providing both data inputs and acting on recommendations. Evaluation and status reports are reviewed by NYSERDA's Senior Management prior to being finalized.

## SECTION 5: RADIOACTIVE WASTE MANAGEMENT

### Primary Functions

- Management of NYSERDA's activities in the West Valley Demonstration Project (WVDP)
- Management of the State Licensed Disposal Area and Retained Premises of the Western New York Nuclear Service Center (WNYNSC)

### Controls

**The West Valley Demonstration Project Act - T**he WVDP Act directs the U.S. Department of Energy (DOE) to carry out a demonstration project on high-level radioactive waste solidification and decommissioning at the WNYNSC. The WVDP Act directs DOE and NYSERDA to enter into a Cooperative Agreement to carry out the WVDP. The WVDP Act also stipulates that the federal government will pay 90 percent of the WVDP costs and New York State will pay 10 percent.

**Cooperative Agreement Between United States Department of Energy and New York State Energy Research and Development Authority on the Western New York Nuclear Service Center at West Valley, New York -** The Cooperative Agreement lays out a framework between DOE and NYSERDA on the implementation of the WVDP. The Agreement stipulates that DOE has the sole responsibility for carrying out the Project, but also provides for continued consultation and coordination between DOE and NYSERDA during the conduct of the WVDP. The Cooperative Agreement also provides for NYSERDA's participation in DOE's procurement process for selecting the management and operations contractor for the WVDP. NYSERDA provides DOE with input on WVDP activities, progress, plans, funding, issues and concerns, and participates in WVDP meetings with the public, regulators, technical consultants and experts and other stakeholders.

**Consent Decree** - The Consent Decree, filed with and approved by the U.S. District Court, resolves the majority of claims brought in a lawsuit filed by NYSERDA and New York State against DOE and the federal government regarding cost allocation for cleanup at the WNYNSC. In addition to the 90/10 cost split identified in the WVDP Act and the Cooperative Agreement for WVDP facilities, the Consent Decree identifies a specific cost split between NYSERDA and DOE for all remaining facilities and contamination at the WNYNSC. The Consent Decree is implemented in accordance with a Consultation Agreement prepared by DOE and NYSERDA.

**Waste and Facilities Management Committee -** The West Valley Site Management Program reports to NYSERDA's Board through its Waste and Facilities Management Committee. The Waste and Facilities Management Committee is provided with routine updates on WVSMP activities, accomplishments, issues, and other noteworthy items. The Committee provides guidance to the West Valley Site Management Program in regard to West Valley activities for the WVDP and the State License Disposal Area (SDA). The Chair of the Committee reports on the West Valley program to the full Board.

**Regulatory Requirements** – Work performed at the SDA is subject to numerous regulatory requirements and mechanisms, including a Radioactive Materials License issued by the NYS Department of Health, a Radiation Control Permit and a State Pollutant Discharge Elimination System permit issued by the New York State Department of Environmental Conservation, and a Consent Order issued by the NYS Department of Environmental Conservation and the U.S. Environmental Protection Agency. NYSERDA must also comply with all other applicable State and federal regulations, including regulations for

hazardous waste generation, management, and disposal; worker industrial safety; wetland protection; and environmental review.

**Written Plans and Procedures** – Written plans and procedures provide the mechanism for implementing the regulatory requirements identified above and for implementing additional best management practices. Plans and procedures are prepared by technical staff or contractors, and are reviewed and approved by the SDA Program Manager before they are incorporated into the program for implementation. Radiation Safety and Health and Safety plans and procedures are also reviewed and approved by the Team Lead and Radiation Safety Committee or Safety Committee before they are incorporated into the program for implementation.

**Radiation Safety Committee –** The WVSMP Radiation Safety Committee oversees the WVSMP's Radiation Protection Program, ensuring that all individuals who work with, or in the vicinity of radioactive materials at the SDA have sufficient training and experience to perform their duties safely and in accordance with applicable NYS Department of Health regulations and the Radioactive Materials License. The Radiation Safety Committee also ensures that all uses of radioactive materials at the SDA is conducted in a safe manner and in accordance with applicable regulations.

**Safety Committee** – The West Valley Site Management Program Safety Committee oversees the WVSMP Health and Safety Program to establish policies, administrative controls and procedures to protect workers at the SDA and other NYSERDA-controlled areas of the WNYNSC in accordance with applicable Occupational Safety and Health Administration and NYS Department of Labor regulations. The Safety Committee also provides guidance to the Safety and Health Supervisor on the implementation of the Safety and Health Program.

**Project Initiation Request Committee** – The Project Initiation Request Committee reviews all potential contract actions at an early stage to provide initial WVSMP management review and input on all activities requiring NYSERDA contract actions, in accordance with NYSERDA Contracting Guidelines requirements. The Committee evaluates and provides input on the purpose and need for the activity, the contracting approach, funding considerations, resource needs and availability, and staff involvement.

## SECTION 6: BOND FINANCING

### Primary Functions

- Issue tax-exempt bonds for utilities and other qualifying entities to finance eligible facilities
- Administer utility bonds previously issued

### Controls

Issue tax-exempt bonds for qualified entities to finance eligible facilities

Proposed financings are reviewed for eligibility by both NYSERDA staff and independent bond counsel.

An intent to issue new tax-exempt bonds may initially be evidenced by the approval of an inducement resolution or declaration of intent by the Audit and Finance Committee of NYSERDA's Board. The purpose of the inducement resolution or declaration of intent is to preserve, under the Federal Internal Revenue Code, the eligibility of the costs incurred from the date the action is taken to the date of the future financing for tax-exempt status.

New financings and refunding's also require the approval of an implementing resolution adopted by NYSERDA's Board.

### In addition to NYSERDA Approval:

- The State Comptroller must approve bonds issued through a private negotiation sale, instead of public bid. As Chair of the State Securities Coordinating Committee, the Comptroller also oversees scheduling of major State and public authority financings.
- The Commissioner of the Department of Taxation and Finance approves certain arrangements of a bond sale, such as procedures for the security, collection, and investment of bond proceeds.
- The Public Authorities Control Board (PACB) reviews and approves the adequacy of the financial security of the bond issue.
- The Governor approves the minutes of NYSERDA's Board meetings. The Internal Revenue Code, also requires the Governor's approval for new bond financings that qualify as private activity bonds.

Administer bonds previously issued

The Finance Department prepares billings for annual administrative fees as summarized in the bond documents.

## SECTION 7: CONTRACTS MANAGEMENT

### Primary Functions

- Manage procurement and contracting process
- Contract management and administration

### Controls

Manage procurement and contracting process

The Director of Contract Management approves all procurements and contracts and ensures that they are consistent with NYSERDA's Contracting Guidelines and applicable Executive Orders and other requirements.

The Director of Contract Management reports to the Board on NYSERDA's compliance with the Contracting Guidelines as specified in those guidelines.

Duties are segregated between procurement, contract negotiation, and contract execution.

NYSERDA maintains standard contract terms and conditions. Significant exceptions to terms and conditions are identified for contract execution.

Contract Management staff provide training to staff on procurement and contracting policies and procedures to ensure compliance.

Each solicitation issued by the Authority shall designate the person(s) who may be contacted by offerers related to procurement pursuant to Section 139-j of the State Finance Law. Generally, any communication from an outside party which could reasonably be considered an attempt to influence the procurement may only be made to the designated person(s) in the solicitation.

Contract management and administration

The Contracts Management unit maintains central files including solicitations and contractual agreements.

The Contract Management unit is responsible for verifying compliance with contractual obligations, particularly provision for insurance and recoupment.

## SECTION 8: ACCOUNTING

### Primary Functions

- Preparation and approval of annual Budget and Financial Plan
- Maintenance of accounting records and systems and preparation of financial statements
- Cash and investments management
- Revenue processing
- Payment processing
- Payroll Processing
- Fixed assets

### Controls

Preparation and approval of annual Budget and Financial Plan

A proposed Budget and Financial Plan are initially prepared by Authority staff in accordance with generally accepted accounting principles on a modified accrual basis. Included are a corresponding proposed Budget and Financial Plan prepared on a cash basis, based on reasonable assumptions and methods of estimation. They are presented in a manner consistent with the Authority's programs and functions and include detailed estimates of revenues and expenditures for each program or function.

The proposed Budget and proposed Financial Plan are made available for public inspection, through posting on NYSERDA's website, no less than 60 days before the start of the fiscal year and at least 30 days before approval by the Board Members.

NYSERDA's proposed Budget and proposed Financial Plan are accompanied by:

- a description of the budget process, including the dates of key Budget decisions;
- a description of the principal Budget assumptions, including sources of revenues, staffing and future collective bargaining costs, and programmatic goals;
- a self-assessment of budgetary risks;
- a revised forecast of the current year's budget;
- a reconciliation that identifies changes in estimates from the projections in the previously approved budget and financial plan;
- a statement of the last completed fiscal year's actual financial performance in categories consistent with the proposed budget or financial plan
- a projection of the number of full-time and full-time equivalents employees, including sources of funding, and functional classifications;
- a statement of each revenue-enhancement and cost-reduction initiative that represents a component of any gap-closing program and the annual impact on revenues, expenses and staffing;
- a statement of the source and amount of any material non-recurring resource that is planned for use in any given fiscal year;
- a statement of any transactions that shift material resources from one year to another and the amount of any reserves;
- a statement of borrowed debt projected to be outstanding at the end of the fiscal year covered by the proposed Budget or proposed Financial Plan, the planned use or purpose of debt issuances,

scheduled debt service payments for both issued and proposed debt, the principal amount of proposed debt and assumed interest rate(s), debt service for each issuance as a percentage of total pledged revenues listed by type or category of pledge revenues, cumulative debt service as a percentage of available revenues, and the amount of debt that can be issued until legal limits are met;

- a statement of the annual projected capital cost broken down by category and sources of funding, and for each capital project, estimates of the annual commitment, total project cost, expected date of completion and the annual cost for operating and maintaining those capital projects or capital categories that, when placed into service, are expected to have a material impact on the operating budget; and
- a certification by the President and CEO that, to the best of his or her knowledge and belief after reasonable inquiry, the proposed Budget and proposed Financial Plan are based on reasonable assumptions and methods of estimation.

As part of the annual budget process, NYSERDA staff prepare working papers that detail the assumptions and methods of estimation used in preparing the proposed Budget and proposed Financial Plan.

The proposed Budget and Financial Plan are then submitted to NYSERDA's Board Members for approval in accordance with Section 2801 of the Public Authorities Law. After approval, the approved Budget and Financial Plan are submitted to the persons designated in such Section 2801 to receive such Budget and Financial Plan. This includes submitting copies of the approved Budget and Financial Plan to the State Comptroller within 7 days of approval by the Board Members, subject to approval by the Governor pursuant to Section 1854 of the Public Authorities Law. The approved Budget and Financial Plan are also made available for public inspection, through posting on NYSERDA's website, not less than 7 days before the start of the fiscal year.

Thereafter, the Treasurer provides quarterly updates to the Board Members on the status of actual revenues and expenses compared to the Budget targets. The Treasurer also provides the Board Members with a written mid-year report to explain and quantify material variances that are due to timing or have a budgetary impact, and provide an assessment of the impact. The report includes the status of capital projects, including but not limited to commitments, expenditures and completions, and an explanation of material cost overruns and delays. Subsequent changes to the Budget and the Financial Plan are made, as required, subject to approval by the Board Members.

Through posting on NYSERDA's website, not less than 90 days after the close of each fiscal year, the Treasurer publicly posts actual versus estimated Budget results as reported in NYSERDA's audited financial statements. The Treasurer also notifies the Board Members and the State Comptroller, in writing, at any point during the fiscal year when he or she learns of any adverse development that would materially affect the Budget or Financial Plan.

Maintenance of accounting records and systems and preparation of financial statements

As required by statute, NYSERDA's annual financial statements, which are prepared in accordance with generally accepted accounting principles and accounting standards promulgated by the Governmental Accounting Standards Board, are audited by independent auditors selected by the Audit and Finance Committee and the Board. In addition, the Treasurer provides quarterly financial statements to the Board, including a comparison of actual results against budgeted amounts. Expenditure statements are also provided quarterly to Program Directors, Program Managers and department heads.

Accounting, through a third-party service provider, prepares, reviews and/or signs tax reporting forms (eg., payroll/employment taxes, informational reporting of exemptions, taxable fringe benefits and other payments) required by Federal, State and local regulations.

NYSERDA ensures compliance with Federal, State, and Local tax reporting obligations of NYSERDA. In addition, NYSERDA solicits a tax compliance review from an independent accounting firm as deemed necessary, but not less than once every three years, to review NYSERDA's compliance with applicable tax regulations.

Cash and investments management

The Commissioner of Taxation and Finance serves as fiscal agent to NYSERDA pursuant to statute. There are no funds under NYSERDA's direct control. The fiscal agent, at the direction of NYSERDA, actually purchases, sells, and retains custody, where appropriate, of NYSERDA investments.

NYSERDA is subject to the provisions of Public Authorities Law Section 2925, the Office of the State Comptroller's "Investment Guidelines for Public Authorities," the provisions of NYSERDA's enabling legislation concerning NYSERDA investments, and NYSERDA's own "Investment Guidelines, Operative Policy and Instructions." At least annually, the Audit and Finance Committee of NYSERDA's Board reviews and evaluates NYSERDA's investment program results and approves any revisions to the Guidelines.

Duties are segregated between receipt and custody, depositing, recording, and reconciling cash and checks received.

The purchase and sale of investments is authorized by the Treasurer (or in his/her absence, the Controller and Assistant Treasurer, or any NYSERDA Officer), according to policy guidelines. Duties are segregated between authorization and recording of investments.

Receipts are deposited promptly, generally weekly.

The fiscal agent reconciles cash and investment accounts monthly. NYSERDA staff independently reconcile this data with the accounting records.

Revenue processing

Proper segregation of duties exists in the initiation, recording, and reconciliation of revenues. Only Accounting staff not responsible for cash reconciliations or deposits are authorized to prepare invoices.

A list of outstanding invoices is produced monthly and reconciled with the general ledger. Notices are sent for any outstanding invoices more than 30 days past due. The Controller and Assistant Treasurer, with the assistance of the Senior Energy Accountant, is responsible for following up on delinquent accounts.

An account receivable may only be written-off after all reasonable collection efforts have been exhausted and requires the approval of the Controller and Assistant Treasurer or any other NYSERDA Officer. The Controller and Assistant Treasurer or any other NYSERDA Officer must also approve any deferred

payment arrangements.

Accounts receivable more than 120 days past-due may be submitted to a private collection agency or the Attorney General's Office for collection.

As an alternative to receiving payments from RD&D program contractors through recoupment, and in an effort to assist in growing small businesses, NYSERDA may instead elect to take an equity position in an RD&D contractor. When deemed appropriate, an equity investment is consummated through a negotiated Stock Purchase Agreement, which outlines the terms and conditions of NYSERDA's investment.

Payment processing

Section 2880 of the Public Authorities Law requires that payment be made to vendors within 30 days on all valid invoices. Failure to do so will result in the payment of interest.

Accounting staff prepares a weekly report of outstanding vouchers and their due dates which is reviewed by the Controller or Treasurer. NYSERDA reports annually to the Board at the June meeting on its compliance with the prompt payment policy.

Prior to payment, proper authorization must exist for payments to contractors.

All contracts or purchase orders must be signed by an Officer. Contracts or agreements in excess of $1,000,000 must be signed by the President and CEO. Generally, goods and services in excess of $5,000 require a written contract or purchase order.

Accounting staff monitor all payments, assuring that all invoices are mathematically correct, contain proper documentation, are within authorized funding limits, and are in accordance with the terms and conditions of the contract or purchase order.

Additional approval for payment is required from the Project Manager for payments under program contractual agreements, or from the Program Manager or department head, for administrative costs. Invoices equal to or greater than $500,000 require secondary approval by the initial approvers' Supervisor.

NYSERDA checks require the signature of the Commissioner of Taxation and Finance, NYSERDA's fiscal agent. Payees electing to receive payment from NYSERDA by electronic transfer provide the necessary information and authorization in writing. Approval for disbursements is noted on a warrant request, which must be signed by an authorized signatory: the Controller and Assistant Treasurer or any NYSERDA Officer. For payees receiving payment by electronic transfer, the automated accounting system produces an electronic file containing necessary banking information for payees, which is transmitted to the bank by NYSERDA Finance staff and later released for processing to the bank by the Department of Taxation and Finance after all their reviews have been completed.

NYSERDA's integrated financial management system provides for automated, role-based security that properly segregates user access to functions for vendor accounting information addition and maintenance, invoice entry, invoice approval, and payment preparation. In addition, the system's budgetary management system prevents expenditure or encumbrance of funds in excess of authorized program funding.

Payroll Processing

NYSERDA's President and CEO, or designee authorizes in writing payroll additions or salary changes. The Director of Human Resources provides notice, in writing, of any salary deletions. Human Resources staff initiates all ministerial changes such as benefit changes in accordance with requests submitted by employees.

All employees are required to maintain daily time records on a bi-weekly basis, using the automated time and attendance system. Employee timesheets require approval by the individual's supervisor.

NYSERDA uses a computerized payroll system to calculate and process payroll and checks. Access to the system is password restricted to only those individuals in the Accounting unit with responsibility for processing payroll.

Fixed assets

Accounting staff maintain a computerized fixed asset system, ensuring that all fixed assets are identified by location, and that the fixed asset ledger is reconciled to the general ledger. Only assets with a dollar value in excess of $2,500 and a useful life greater than two years are recorded.

The disposition of real property and personal property shall be in accordance with the Guidelines, Operative Policy, and Instructions for the Disposal of Real and Personal Property. The Treasurer is responsible for ensuring compliance with these guidelines, including the preparation of an annual report listing all real property of the Authority and a description of all real and personal property disposed of during such period.

Financial Statements

NYSERDA prepares annual financial statements in accordance with generally accepted accounting principles (GAAP) applicable to state and local government entities, which are approved by the Board at the June meeting. The annual financial statements include a comparison of actual results versus financial projections and a certification by the Officers and the Director of Internal Audit that the financial statements and disclosures fairly present, in all material respects, the operations and financial condition of NYSERDA. NYSERDA's most recent annual financial statements are made available on the NYSERDA web site. Interim quarterly financial statements are also provided to the Board.

Financial statements are audited by an outside independent accounting firm selected by the Audit and Finance Committee and Board. The independent auditors are selected in accordance with the requirements of Section 2802 of the Public Authorities Law and are prohibited from providing non-audit services to NYSERDA contemporaneously with the audit, except as provided in Section 2802 of the Public Authorities Law. Non-audit services include bookkeeping or other services related to the accounting records or financial statements of NYSERDA; financial information systems design and implementation; appraisal or valuation services, fairness opinions or contribution-in-kind reports; actuarial services; internal audit outsourcing services; management functions or human services; broker or dealer, investment advisor, or investment banking services; and legal services and expert services unrelated to the audit.

The independent auditors must timely report to the Audit and Finance Committee all critical accounting policies and practices to be used, all alternative treatments of financial information within generally

accepted accounting principles that have been discussed with Authority management officials, ramifications of the use of such alternative disclosures and treatments, and the treatment preferred by the certified independent public accounting firm; and other material written communications between the independent auditors and NYSERDA management, such as the management letter along with management's response or plan of corrective action, material corrections identified or schedule of unadjusted differences, where applicable.

The audit partner or lead audit partner responsible for reviewing the audit must not have performed audit services for the Authority in each of the five previous fiscal years.

## SECTION 9: HUMAN RESOURCES

### Primary Functions

- Recruit employees
- Manage compensation functions to appropriately reward employees
- Manage performance programs to reinforce and correct behaviors
- Manage employee benefits programs
- Facilitate employee training

### Controls

Recruit employees: Prohibited Actions

All NYSERDA positions are filled based on merit. A position posting containing minimum education and skill levels are established for every position. Reference, employment, criminal background and education information is verified for all prospective employees. The President and CEO, Treasurer, or Director of Internal Audit cannot have been employed by the Authority's independent auditors during the two-year period preceding an audit.

NYSERDA employees and board members are prohibited from participating in any hiring or employment decision or any contracting decision relating to any relative, and no employee may be hired into a position that reports to a relative.

No employee involved in recruiting, interviewing, or hiring applicants for employment or making promotional, disciplinary, or other employment decisions may ask any such applicant or employee to reveal their party affiliation, whether he or she has made campaign contributions, or whether the candidate voted for any elected official or candidate for elective office.

Manage compensation functions to appropriately reward employees

Merit payment recommendations are reviewed and approved by the Director of Human Resources and the Officers for conformance with NYSERDA's policies.

Manage performance programs to reinforce and correct behaviors

An annual Performance Review is drawn up between each employee and employee's supervisor which summarizes the employee's job responsibilities and specific performance objectives which are used for the performance evaluation. The document also summarizes planned training and development activities.

Performance Improvement Plans are completed by supervisors and approved by Human Resources for employees whose performance warrants significant improvement.

Manage employee benefits programsHuman Resource staff provides assistance to employees with enrollment, changes, or answering questions for various NYSERDA-sponsored employee benefit programs.Special benefits, such as flexible work hours or part-time work are evaluated on a case-by-case basis with approval from the employee's supervisor and the Director of Human Resources to ensure consistent and equitable application.

Faciliate employee training

Human Resources facilitates various Statewide mandatory as well as other Authority-wide employee training programs using internal and external trainers. Individual employee training and professional development needs are generally identified as part of the evaluation process. Requests are approved by the direct supervisor, Team Lead, and Director of Human Resources.

## SECTION 10: INFORMATION TECHNOLOGY

### Primary Functions

- Procure, operate and maintain computer hardware and software
- Maintain security of computer hardware and software
- Provide training to staff on computer hardware and software usage
- Maintain Authority Web Site

### Controls

Procure, operate and maintain computer hardware and software

The Director of Information Technology must approve the purchase of computer hardware or software.

The IT unit maintains a service desk ( help desk) during normal business hours to respond to staff questions and problems with NYSERDA hardware or software.

The IT group contains several governance committees created to review, approval, and prioritize information technology projects. These committees include the following:

1. PeopleSoft (NEIS) – For Financial/Contractual system governance
2. Web – For projects related to web site development either internally or externally
3. Development – For enhancements to existing systems
4. Salesforce – For enhancements and new build requests on the Salesforce platform
5. Data Warehouse – For enhancements, new build and data quality work associated with the data warehouse

Each governance committee contains IT staff, Operational Transformation & Lean, Business unit, and Officer level representation.

All information technology development projects shall conform with system development life cycle standards in accordance with New York State policy requirements (NYS-S13-001).

Maintain security of computer hardware and software

All electronic data stored on the network file server is automatically backed up on a nightly basis. Once daily a copy of the backup is transmitted to an off-site server where up to 30 days of backups are retained. On a quarterly basis, a long-term backup is dropped to disk and stored off-site in a fireproof safe.

Staff are encouraged to store any data considered critical to the operation of NYSERDA on the network server, rather than on staff personal computers. This allows the data to become part of the automatic backup and disaster recovery procedures.

Electronic data stored on personal computers is backed up by the staff member to whom the computer is assigned. As an additional level of protection, non-sensitive personal computer backup media can be stored off-site, either at the staff member's home or at NYSERDA's off-site storage locations. This data must be encrypted prior to removal from the premises. The service desk can assist with the process.

Every reasonable effort is taken to ensure access to the network is restricted to valid users, and each user is given a password. The password can be changed by the user at any time or by the system administrator. System integrity is maintained by restricting network user privileges and by centralizing management duties to a password protected system administrator. Only the system administrator can alter network programs, security or operations. Physical access to the network computer systems equipment is limited to authorized staff.

All data stored on the network or personal computers is considered NYSERDA work product. NYSERDA computers and information systems (including email) must be used in accordance with New York State policy requirements (NYS-P14-001).

Recovery from the physical destruction of the network computer system is accomplished by using the most recent backup available and restoring data to another computer network system. At that time, single users can access critical computer-based information until NYSERDA operations can be reestablished at another location. Recovery from personal or network computer failure is accomplished by using spare computers or parts and restoring lost data from backup media. In some situations, accidentally deleted data can be recovered with the use of software utilities available to the system administrator.

Employees may borrow certain equipment for use outside NYSERDA for a finite length of time. The employee must sign the hardware out from the Service Desk Supervisor or his/her designee.

It is NYSERDA's policy to adhere to the stipulations of relevant end user license agreements and the copy protection laws which apply to a software package. Illegal copying of NYSERDA software, or use of illegal copies of software packages on any of NYSERDA's computers, is not permitted. In the event that an illegal copy of software is found on the premises, it will be destroyed immediately.

Non-NYSERDA software may not be copied or installed on NYSERDA computers without written authorization from the Service Desk Supervisor.

Every staff member of NYSERDA is assigned a computer and is given access to the network. It is the responsibility of each staff member to protect NYSERDA's investment in computer technology. The computers and software provided by NYSERDA for staff use are to be used for NYSERDA business purposes only. While employed by NYSERDA, each staff member shall be responsible for all assigned computer items. Staff members shall report immediately any lost, damaged or missing items.

The Information Technology unit records the serial number of each piece of equipment provided to each staff member; maintains a record of manuals and software programs provided to staff members; and updates these records as equipment, manuals and software are added or removed.

As part of the employee exit interview process, the IT Director or designee, signs the Exit Clearance Form, described in NYSERDA's Personnel Handbook, indicating that all assigned computer equipment, manuals and disks have been returned. All discrepancies must be cleared before the final paycheck can be released.

Provide training to staff on computer hardware and software usage

Information Technology unit staff conduct one-on-one or group training on various software applications and computer technology or can research and recommend outside training when requested.

Maintain Authority Web Site

The Information Technology unit is responsible for maintaining the Authority's web site(s) based on requests approved by the Communication & Corporate Marketing department. At a minimum, the web site shall include a description of NYSERDA's mission, current activities, most recent financial reports, current year budget, its most recent independent audit report, and Guidelines, Operative Policy and Instructions for the Disposal of Real and Personal Property.

## SECTION 11: INFORMATION SECURITY

**Primary Functions**

- Protect and maintain the confidentiality, integrity and availability of information and related infrastructure assets
- Manage the risk of security exposure or compromise
- Assure a secure and stable information technology (IT) environment
- Identify and respond to events involving information asset misuse, loss or unauthorized disclosure
- Monitor systems for anomalies that might indicate compromise
- Promote and increase the awareness of information security

**Controls**

The NYS Office of Information Technology Services (ITS) establishes and regularly updates policies, standards, and guidelines for information security (collectively referred to as "ITS Security Policies") for State Entities, including NYSERDA. These policies apply to all NYSERDA information technology devices and data, regardless of their medium or form. All individuals, including but not limited to, NYSERDA employees, contracts, temporary employees, and interns, who handle NYSERDA information must adhere to the provisions of these policies.

The Information Security Officer is the central point of contact for all information security matters. He or she reports independently to the Treasurer. The duties of the Information Security Officer are segregated from the operation of the information technology systems.

The Information Security Officer is responsible for the design, implementation and monitor of systems and procedures to protect and assure the availability of NYSERDA's information and related infrastructure assets and to monitor for, and respond to, events involving information misuse, loss or unauthorized disclosure.

All data collected and stored by, or on behalf of, NYSERDA are classified and managed per policies and procedures outlined in NYSERDA's Data Classification and Security Controls Policy. NYSERDA's Data Governance Office is responsible for classifying data and coordinating external sharing requests with the Office of the General Counsel and Information Technology. Also, the Data Governance Office ensures that user authorization and permissions are set to protect confidential data.

To protect NYSERDA's computer systems against the introduction or spread of a computer virus, the network server and staff personal computers have been equipped with virus protection software. The virus protection software is configured for automatic checking and system shielding to detect and contain viruses as soon as possible. Network server files are scanned for viruses each time they are used while personal computer files are scanned once per day when the user first logs onto the LAN. The virus protection software also enables staff to manually scan hard drives, USB Drives, and CD's as needed. In addition, portable computers that are signed out are scanned upon being returned.

All NYSERDA employees are required to complete annual state cyber security training.

## SECTION 11: COUNSEL'S OFFICE

### Primary Functions

- Provides legal advice and drafts legal opinions and documents for NYSERDA.
- Provides legal advice and oversight of the contracting process
- The Office of the General Counsel provides guidance to the Communications department in responding to Freedom of Information Law (FOIL) requests.
- Renders advice concerning all NYSERDA programs and policies
- As designated by the President and CEO, a Counsel's Office attorney serves as NYSERDA's ethics officer.
- Reviews NYSERDA related proposed legislation and regulations by providing assistance to the Governmental Affairs Director.
- Assists in the drafting of NYSERDA's rules and regulations and reviews NYSERDA's applications for permits and environmental assessments.
- Performs the secretarial function for the standing committees of the Board.
- Coordinates NYSERDA records management systems

### Controls

Provides legal advice for all NYSERDA matters.

General Counsel represents NYSERDA's interests in legal actions or proceedings and consults with executive management as deemed necessary.

Upon receipt of notice that an offerer has made contact with someone other than the Designated contact with respect to a procurement for a reason inconsistent with subsection 3 of Section 139-j of the State Finance Law, the ethics officer will immediately investigate the allegation, in accordance with the procedures set forth in, and make a determination as required by, such Section 139-j. A finding that an offerer has knowingly and willfully violated subsection 3 of Section 139-j of the State Finance Law will result in a finding of non-responsibility for such offerer as required by such section.

NYSERDA's President and CEO designates a Records Management Officer and has currently designated a member of Counsel's Office to act in that capacity. In consultation with the New York State Archives, the Records Management Officer is tasked with implementing the records management system, and providing staff with guidelines for maintaining records.

As part of the records management system, NYSERDA has adopted the General Retention and Disposition Schedule for New York State Government Records as issued by the New York State Archives Government Records Services. No record may be destroyed without the express consent of the Records Management Officer in accordance with the General Retention and Disposition Schedule for New York State Government Records, which is located on NYSERDA's intranet.

## SECTION 12: GOVERNMENTAL AFFAIRS

### Primary Functions

- To serve as a liaison between NYSERDA and all elected officials
- To address inquiries from the Governor's office, members of the federal and State legislature, as well as local government officials

### Controls

Records

The Office of Governmental Affairs tracks federal and State legislation that directly impacts energy-efficiency and environmental conservation policies, as well as legislation that may have other potential implications for NYSERDA and its stakeholders. Additionally, staff monitors legislative hearings, assists with the preparation of testimony for hearings, and coordinates the management of NYSERDA's legislative agenda.

The Director of External Affairs will maintain all records of contacts, whether oral or written, that are an attempt to influence the adoption or rejection of any rule or regulations having the force and effect of law that is issued by NYSERDA.

## SECTION 13: COMMUNICATIONS

### Primary Functions

- Responds to media and public inquiries on programs and acts as a liaison to the Governor's Press and Scheduling Offices
- Issues news releases, arranges media events, and oversees social media accounts
- Responsible for responding to Freedom of Information Law (FOIL) requests with guidance from Counsel's Office

### Controls

Responds to media and public inquiries on programs

Staff receiving phone calls, messages or other inquiries from the print or electronic media (including free-lance journalists or reporters) are required to immediately forward such inquiries to Communications staff for response. As appropriate, Communications staff discusses responses with technical, legal, contracts, or administrative staff.

Issues news releases, arranges media events
and oversees social media accounts

Communications staff are responsible for press releases regarding NYSERDA news, events, and programs. Communications works with the staff responsible for programs or events to draft a press release. Press releases are reviewed and approved by the Director of Communications (or designee), the President and CEO, and other parties involved.

Communications staff review NYSERDA-funded projects with special attention to the technology transfer components. Communications staff work with staff from other departments on technology transfer efforts that require communications expertise.

Communications staff are also responsible for targeting information to appropriate audiences-internal and external- to maximize the effectiveness of NYSERDA's outreach efforts.

All social media content distributed by NYSERDA across its various social media platforms is overseen by the Digital Content Editor and Social Media Manager who report into the Director of Communications.

Responding to Freedom of Information Requests

The Director of Communications assigns and oversees a Records Access Officer to respond to Freedom ofInformation Law (FOIL) requests with guidance from the Office of the General Counsel.

## SECTION 14: CORPORATE MARKETING

### Primary Functions

- Oversee execution of brand standards and visual guidelines across all NYSERDA communications
- Work with program staff, leading the development and execution of marketing plans
- Coordinate activities with assigned Communications, Social Media, and Web staff
- Develop messaging to ensure consistency in market
- Produce marketing materials and publications
- Oversee electronic communications sent via Salesforce CRM
- Produce and distribute general and technical reports about NYSERDA and its programs

Work follows one of two paths:

- Marketing works with competitively selected marketing firm to plan and implement a program to meet business objectives. This work is funded through program budgets.
- Marketing Services, an in-house marketing resource, creates materials, presentations, case studies, and other materials to support marketing of an identified initiative.

### Controls

Marketing materials and publications

Marketing staff work with executive and program staff to produce effective marketing materials (reports, brochures, case studies and fact sheets, paid advertising, displays, direct mail, exhibits, videos, presentations, conference materials, website content, and marketing collateral). Materials are reviewed and approved by an identified list of approvers for each project. Staff coordinate and monitor external mailings, NYSERDA photography and content.

## SECTION 15: CONSUMER SERVICES AND EVENTS MANAGEMENT

### Primary Functions

- Provide consumer information
- Manage and coordinate NYSERDA marketing events

### Controls

Consumer Services

The department manages the contract for NYSERDA's toll-free telephone inquiry line for consumer information operated by an outside contractor. Staff maintains up-to-date knowledge of NYSERDA's initiatives and eligibility criteria to train and support contract staff as well as respond directly to questions and inquires as necessary.

Events Management

Staff identify appropriate events, conferences, and exhibit opportunities for NYSERDA program marketing, outreach, and education, and provide conference and meeting support including venue selection and contracting, equipment and facility logistics. The department maintains a NYSERDA-wide events calendar to provide for coordination of activities.

## SECTION 16: INTERNAL AUDIT

The Authority shall maintain an internal audit function, consistent with Public Authorities Law Section 2932.

**Purpose and Mission**
The purpose of the Authority's internal audit function is to provide independent and objective assurance and consulting services designed to add value and improve the Authority's operations, and, consistent with Public Authorities Law Section 2932, evaluate the Authority's internal controls and operations, identify internal control weaknesses that have not been corrected and make recommendations to correct these weaknesses. The mission of internal audit is to enhance and protect organizational value by providing risk-based and objective assurance, advice, and insight. This is to be accomplished through a systematic, disciplined approach of evaluating the effectiveness of, and, when appropriate, recommending improvements to risk management, control, and governance processes.

**Standards for the Professional Practice of Internal Auditing**
The internal audit function will govern itself by adherence to the mandatory elements of The Institute of Internal Auditors' International Professional Practices Framework, including the Core Principles for the Professional Practice of Internal Auditing, the Code of Ethics, the *International Standards for the Professional Practice of Internal Auditing (*the *Standards),* and the Definition of Internal Auditing. The Director of Internal Audit will report periodically to senior management and the Audit and Finance Committee regarding the internal audit function's conformance to the Code of Ethics and the *Standards*.

**Organization, Reporting Structure and Authority**
The internal audit function shall be directed by a chief audit executive ("Director of Internal Audit"), who shall be appointed by the Board Members, as determined by the Audit and Finance Committee. Selection of the Director of Internal Audit shall be based upon his or her internal auditing credentials, including knowledge, skills, experience, and professional certifications necessary to perform the responsibilities described in this section.

The Director of Internal Audit shall report functionally to the Authority's Audit and Finance Committee and administratively (i.e., day-to-day operations) to the President and CEO. To establish, maintain, and assure that the Authority's internal audit function has sufficient authority to fulfill its duties, the Audit and Finance Committee will:

- Approve the internal audit function's description in this Section.
- Approve the risk-based internal audit plan.
- Provide input to the Director of Internal Audit for the internal audit function's budget and resource plan.
- Receive communications from the Director of Internal Audit on the internal audit function's performance relative to its plan and other matters.
- Approve the appointment or dismissal of the Director of Internal Audit.
- Make appropriate inquiries of management and the Director of Internal Audit to determine whether there are inappropriate scope or resource limitations.

The Chair of the Audit and Finance Committee will consult with the President and CEO on the performance reviews and compensation of the Director of Internal Audit.

The Director of Internal Audit shall have unrestricted access to, and communicate and interact directly with the Audit and Finance Committee.

The Audit and Finance Committee authorizes the internal audit function to:

- Have full, free, and unrestricted access to all functions, records, property, and personnel pertinent to carrying out any engagement, subject to accountability for confidentiality and safeguarding of records and information.
- Allocate resources within budgets approved by the board, set frequencies, select subjects, determine scopes of work, apply techniques required to accomplish audit objectives, and issue reports.
- Obtain assistance from the necessary personnel of the Authority, as well as other specialized services from within or outside the Authority, in order to complete the engagement.

**Independence and Objectivity**

The Director of Internal Audit will ensure that the internal audit function remains free from all conditions that threaten the ability of internal auditors to carry out their responsibilities in an unbiased manner, including matters of audit selection, scope, procedures, frequency, timing, and report content. If the Director of Internal Audit determines that independence or objectivity may be impaired in fact or appearance, the details of the impairment will be disclosed to appropriate parties.

Internal auditors will maintain an unbiased mental attitude that allows them to perform engagements objectively and in such a manner that they believe in their work product, that no quality compromises are made, and that they do not subordinate their judgment on audit matters to others.

Internal auditors will have no direct operational responsibility or authority over any of the activities audited. Accordingly, internal auditors will not implement internal controls, develop procedures, install systems, prepare records, or engage in any other activity that may impair their judgment, including:

- Assessing specific operations for which they had responsibility within the previous year.
- Performing any operational duties for the Authority or its affiliates.
- Initiating or approving transactions external to the internal audit function.
- Directing the activities of any Authority employee not employed by internal audit, except to the extent that such employees have been appropriately assigned to auditing teams or to otherwise assist internal auditors.

Where the Director of Internal Audit has or is expected to have roles and/or responsibilities that fall outside of internal auditing, safeguards will be established to limit impairments to independence or objectivity.

Internal auditors will:

- Disclose any impairment of independence or objectivity, in fact or appearance, to appropriate parties.
- Exhibit professional objectivity in gathering, evaluating, and communicating information about the activity or process being examined.

- Make balanced assessments of all available and relevant facts and circumstances.
- Take necessary precautions to avoid being unduly influenced by their own interests or by others in forming judgments.

The Director of Internal Audit will confirm to the Audit and Finance Committee, at least annually, the organizational independence of the internal audit function.

The Director of Internal Audit will disclose to the Audit and Finance Committee any interference and related implications in determining the scope of internal auditing, performing work, and/or communicating results.

**Scope of Internal Audit Activities**

The scope of internal audit activities encompasses, but is not limited to, objective examinations of evidence for the purpose of providing independent assessments to the Audit and Finance Committee, management, and outside parties on the adequacy and effectiveness of governance, risk management, and control processes for the Authority. Internal audit assessments include evaluating whether:

- Risks relating to the achievement of the Authority's strategic objectives are appropriately identified and managed.
- The actions of the Authority's officers, directors, employees, and contractors are in compliance with the Authority's policies, procedures, and applicable laws, regulations, and governance standards.
- The results of operations or programs are consistent with established goals and objectives.
- Operations or programs are being carried out effectively and efficiently.
- Established processes and systems enable compliance with the policies, procedures, laws, and regulations that could significantly impact the Authority.
- Information and the means used to identify, measure, analyze, classify, and report such information are reliable and have integrity.
- Resources and assets are acquired economically, used efficiently, and protected adequately.

The Director of Internal Audit will report periodically to senior management and the Audit and Finance Committee regarding:

- The internal audit function's purpose, authority, and responsibility.
- The internal audit function's plan and performance relative to its plan.
- The internal audit function's conformance with The Institute of Internal Auditor's Code of Ethics and *Standards*, and action plans to address any significant conformance issues.
- Significant risk exposures and control issues, including fraud risks, governance issues, and other matters requiring the attention of, or requested by, the Audit and Finance Committee or the Board.
- Results of audit engagements or other activities.
- Resource requirements.
- Any response to risk by management that may be unacceptable to the Authority.

The Director of Internal Audit also coordinates activities, where possible, and considers relying upon the work of other internal and external assurance and consulting service providers as needed. The internal audit function may perform advisory and related client service activities, the nature and scope of which will be agreed with the client, provided the internal audit function does not assume management responsibility.

Opportunities for improving the efficiency of governance, risk management, and control processes may be identified during engagements. These opportunities will be communicated to the appropriate level of management.

**Responsibility**

The Director of Internal Audit has the responsibility to:

- Submit, at least annually, to senior management a risk-based internal audit plan.
- Submit, at least annually, to the Audit and Finance Committee a risk-based internal audit plan for review and approval.
- Communicate to senior management and the Audit and Finance Committee the impact of resource limitations on the internal audit plan.
- Review and adjust the internal audit plan, as necessary, in response to changes in the Authority's business, risks, operations, programs, systems, and controls.
- Communicate to senior management and the Audit and Finance Committee any significant interim changes to the internal audit plan.
- Ensure each engagement of the internal audit plan is executed, including the establishment of objectives and scope, the assignment of appropriate and adequately supervised resources, the documentation of work programs and testing results, and the communication of engagement results with applicable conclusions and recommendations to appropriate parties.
- Follow up on engagement findings and corrective actions, and report periodically to senior management and the Audit and Finance Committee any corrective actions not effectively implemented.
- Ensure the principles of integrity, objectivity, confidentiality, and competency are applied and upheld.
- Ensure the internal audit function collectively possesses or obtains the knowledge, skills, and other competencies needed to meet the requirements of this Section.
- Ensure trends and emerging issues that could impact the Authority are considered and communicated to senior management, and the Audit and Finance Committee as appropriate.
- Ensure emerging trends and successful practices in internal auditing are considered.
- Establish and ensure adherence to policies and procedures designed to guide the internal audit function.
- Ensure adherence to the Authority's relevant policies and procedures, unless such policies and procedures conflict with this Section. Any such conflicts will be resolved or otherwise communicated to senior management and the Audit and Finance Committee.

- Ensure conformance of the internal audit function with the *Standards*, with the following qualifications:
    - If the internal audit function is prohibited by law or regulation from conformance with certain parts of the *Standards*, the Director of Internal Audit will ensure appropriate disclosures and will ensure conformance with all other parts of the *Standards*.
    - If the *Standards* are used in conjunction with requirements issued by other authoritative bodies, the Director of Internal Audit will ensure that the internal audit function conforms with the *Standards*, even if the internal audit function also conforms with the more restrictive requirements of other authoritative bodies.

**Quality Assurance and Improvement Program**

The internal audit function will maintain a quality assurance and improvement program that covers all aspects of the internal audit function. The Quality Assurance and Improvement Program will include an evaluation of the internal audit function's conformance with the *Standards* and an evaluation of whether internal auditors apply The Institute of Internal Auditors' Code of Ethics. The Quality Assurance and Improvement Program will also assess the efficiency and effectiveness of the internal audit function and identify opportunities for improvement.

The Director of Internal Audit will communicate to senior management and the Audit and Finance Committee on the internal audit function's Quality Assurance and Improvement Program, including results of internal assessments (both ongoing and periodic) and external assessments conducted at least once every five years by a qualified, independent assessor or assessment team from outside the Authority.

## SECTION 17: DISCRETIONARY FUNDS

The expenditure of the Authority's discretionary funds must relate directly to an enumerated power, duty, or purpose of the Authority. Public funds may not be used to purchase items that are considered personal expenses or that are intended to personally benefit a Member, Officer, or employee. The Authority may not use discretionary funds for purchases that are not necessary to advance the mission of the Authority, including supporting the private or personal interests of the Members, Officers, or employees of the Authority.

Examples of inappropriate use of discretionary funds may include, but are not limited to, the purchase of flowers and gifts for Members, Officers, employees, or family members; celebrations for special occasions; charitable contributions or sponsorships; renewal of professional licenses; personal use of Authority vehicles; and costs to purchase or mail holiday cards or expressions of sympathy.

The Authority's handbooks and manuals provide further guidance regarding appropriate uses of the Authority's discretionary funds for expenses directly related to an enumerated power, duty, or purpose of the Authority. The additional guidance sets forth a process for approving discretionary expenditures and indicates the individual authorized to approval such expenditures. The Personnel Handbook contains specific policies regarding reimbursement for food while traveling, professional memberships, use of Authority equipment and vehicles, and tuition reimbursement. The Operations and Procedures Manual details the Authority's policies regarding sponsorships and the purchase of food for meetings and conferences. The Code of Conduct details additional policies regarding use of Authority equipment and vehicles.

# APPENDIX A

## New York State Comptroller Standards for Internal Control in New York State Government
## (Revised March 2016)

## INTRODUCTION

The New York State Governmental Accountability, Audit and Internal Control Act of 1987 (Internal Control Act) required State agencies and other organizations to promote and practice good internal control and to provide accountability for their activities. In 1999, this legislation was made permanent and the State Finance Law was amended to require the State Comptroller to issue internal control standards for State agencies, public authorities and other organizations.

To fulfill this requirement, the State Comptroller developed the internal control standards contained in this publication: Standards for Internal Control in New York State Government. These Standards are based in part on the work of those advocated by leading authorities in the field of internal control, such as the Committee of Sponsoring Organizations of the Treadway Commission (COSO), the U.S. Government Accountability Office (GAO) and other professional organizations. All organizations subject to audit by the Office of the State Comptroller, including State agencies and public authorities, are expected to adhere to these standards, and will be evaluated accordingly in any audits that are performed by that Office.

Internal control is defined as 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. It is the integration of the activities, plans, attitudes, policies, systems, resources and efforts of the people of an organization working together to achieve its mission. Thus, internal control is focused on the mission of the organization, and this mission must be kept in mind when evaluating the appropriateness of specific internal control practices.

The fundamental concepts of internal control are rooted in well-established organizational techniques and practices. The use of these techniques and practices to achieve a strong, effective system of internal control can best be understood within the following conceptual framework: the five basic components of internal control (control environment, information and communication, risk assessment, control activities, and monitoring) and the two supporting activities (strategic planning and internal audit). Each component is composed of key principles representing the fundamental concepts that are suitable for all organizations. A principle that is not present or functioning is deemed to be a "major deficiency" in internal controls. Accordingly, this publication is organized on the basis of this conceptual framework of five internal control components and seventeen related principles, together with two supporting activities.

The application of internal controls is dynamic, and practices that fit past circumstances may need to be adjusted as those circumstances change. To keep yourself informed about developments in the field of internal control and learn what other organizations are doing to meet their internal control needs, you can consult the professional literature, visit relevant websites, join professional accountability organizations, and attend training programs on the subject of internal control. Some of these potential sources of information are listed in the appendix to this publication.

### Part I: New York State's Internal Control Framework

The State of New York is a very large enterprise, with an annual budget around $150 billion and a quarter million employees, as well as over 100 public authorities. It is larger than most of the Fortune 500 companies. Although governments do not seek profits, the responsibility of government officials to protect the taxpayers' money and to use public resources efficiently to serve the people is similar to the responsibility corporate executives have to their shareholders. The similarities between New York State government and big business do not end with economic comparisons. Government and many private sector companies are large organizations with many employees, multiple processes, diverse products and services and numerous customers. In order to succeed, both government and business should manage their operations effectively. While there are many different styles of effective management, there is one common feature among them: attention to internal control and risk management.

Everyone experiences internal control in their daily business activities as well as in their personal lives. Yet it is a subject that is very often misunderstood, ignored or undervalued. Internal control helps bring order, direction and consistency in daily operations and in long-term strategic planning. So, how can a subject of such importance be so unappreciated? The question underscores the need to better define internal control and what it does. This publication is intended to explain to employees of New York State government organizations how internal control plays an important part in their daily work activities.

Most people think that internal controls are about accounting for funds. While that is true, it is a myth that internal controls are only about money. Internal controls are also about demonstrating the value of an entity's programs and reporting its accomplishments. Internal controls are about protecting assets, information, and employees, and enabling the organization to make the best decisions. Internal controls are ingrained in all business systems and functions. They are essential to ensuring that an organization is functioning effectively and efficiently.

Government managers should be able not only to account for funds spent on a program, but also to assess the value of the program and measure its accomplishments. An effective system of internal control can give managers the means to provide accountability for their programs, as well as the means to obtain reasonable assurance that the programs they direct meet established goals and objectives. While managers have a significant impact on an organization's system of internal control, every employee of the organization has a responsibility and a role in ensuring that the system is effective in achieving the organization's mission.

Although an internal control system can vary widely among organizations, the standards for a good system are generally the same. The standards presented in this publication are applicable to all State government organizations, including State agencies and public authorities. You should view them as the minimally acceptable standards for New York State government organizations.

Your existing operations likely already address, at least implicitly, many of the principles and practices that are formalized in these Standards. You should view this information as a guide for evaluating your organization's system of internal control. More information about internal control is available in libraries, from other professional organizations and from experts on the subject, including the Office of the State Comptroller.

## Definition of Internal Control

Many groups and organizations have published standards and guidelines on internal control and defined it in various ways. Each of those definitions has captured the basic concept of internal control using different words. The definitions find common ground in recognizing internal control's extensive scope, its

relationship to an organization's mission, and its dependence on people in the organization.

Internal control is focused on the achievement of the organization's mission. Mission is the organization's reason for existing. It provides a sense of direction and purpose to all members of the organization, regardless of their position, and provides a guide when making critical decisions. Therefore, it is essential that an organization have a clearly stated mission that is known and understood by everyone in the organization. It is also important to understand that, while good internal control will provide "reasonable assurance" that goals and objectives are met, good internal control cannot guarantee organizational success. However, goals and objectives are much less likely to be achieved if internal control is poor.

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.*

In essence, internal control ensures that the right people are using the right systems to accomplish the right thing in the right way.

This definition reflects certain fundamental concepts. Internal control is:

- Geared to achieving objectives in one or more of the following categories—operations, reporting, and compliance.
- A process consisting of ongoing tasks and activities.
- Effected by people—it involves management and staff and the actions they take at every level in an organization, it cannot be reduced simply to policies, procedure manuals, systems, and forms. Internal control will succeed or fail depending on the attention the organization's employees give to it.
- Able to provide reasonable—but not absolute—assurance to an entity's senior management and board of directors.
- Adaptable to the entity structure—flexible in application to the entire entity or to a particular subsidiary, division, operating unit, or business process.

**Three Objectives of Internal Control**

The overall purpose of internal control is to help an organization achieve its mission. There are three types of objectives which emphasize differing aspects of internal control:

- Operations Objectives - pertaining to effectiveness and efficiency of the entity's operations, including operational and financial performance goals. These objectives promote orderly, economical operations and help produce quality products and services consistent with the organization's mission. They also serve to safeguard resources against loss due to waste, abuse, mismanagement, errors and fraud.

- Reporting Objectives - relating to internal and external financial and nonfinancial reporting. These objectives may encompass reliability, timeliness, transparency, or other terms as set forth by regulators, recognized standard setters, or the organization's policies.

- Compliance Objectives - dealing with adherence to laws, regulations, contracts and management directives to which the entity is subject.

**Why Internal Controls are Important**

Internal controls help an organization to achieve its objectives. They are the checks and balances to support the mission while helping prevent fraud, waste, and abuse and ensuring the efficient use of resources. Internal controls are the first line of defense and the best mechanism an organization has to safeguard its assets and resources, even though they can provide only reasonable—not absolute— assurance. All organizations need internal controls to:

- Accomplish their missions;
- Reduce opportunities for fraud;
- Prevent loss of funds or other resources;
- Establish standards of performance;
- Ensure compliance with laws, regulations, policies, and procedures;
- Preserve integrity;
- Avoid bad publicity;
- Ensure public confidence; and
- Protect all employees.

Consequences of weak internal controls can range from inaccurate or incomplete information, to the waste or misuse of assets, and even to embezzlement or theft. One of the most dangerous things about a weak internal control system is that it engenders a lack of accountability. If adverse events occur, such as theft or a severe failure, it can be difficult to identify the specific cause of the problem and determine who may be responsible if accountability is not established. As a result, innocent staff can fall under suspicion. Strong controls can help to identify who or what went wrong, and what corrective actions are needed. On the broader level, a lack of accountability can result in the erosion of public confidence and support, and can also hamper an organization’s ability to serve the public effectively.

**Organizational Roles**

Every member of an organization has a role in the system of internal control. The human factor is critical to the system’s success. Internal controls are developed by people, guide people, and provide them with a means of accountability. People are responsible for implementing each element of the system properly. Individual roles in the system of internal control vary greatly throughout an organization. Very often, an individual's position in the organization determines the extent of that person's involvement in internal control.

The strength of the system of internal control is dependent on people's attitudes toward internal control and their attention to it. Executive management needs to set the organization’s "tone” regarding internal control. If executive management does not establish strong, clearly stated support for internal control, the organization as a whole will most likely not practice good internal control. Similarly, if individuals responsible for control activities are not attentive to their duties, the system of internal control will not be

effective. People can also deliberately defeat the system of internal control. For example, a manager can override a control activity because of time constraints, or two or more employees can act together in collusion to circumvent control and "beat the system." To avoid these kinds of situations, the organization should continually monitor employee activity and emphasize the value of internal control.

While everyone in an organization has responsibility for ensuring the system of internal control is effective, the greatest amount of responsibility rests with the managers of the organization. Management has a role in making sure that all employees have the necessary skills and capacities and in providing employees with appropriate supervision, monitoring, and training to reasonably ensure that the organization has the capability to carry out its work. The organization's top executive, as the lead manager, has the ultimate responsibility. The Internal Control Act provides that the top executive is responsible for establishing the organization's system of internal control, and is also responsible for: (1) establishing a system of internal control review; (2) making management policies and guidelines available to all employees; and (3) implementing education and training about internal control and internal control evaluations. To the extent that the top executive authorizes other managers to perform certain activities, those managers become responsible for those portions of the organization's system of internal control.

The law further requires the head of the organization to designate an internal control officer who reports to him or her. The Internal Control Officer should be an individual with sufficient authority to act on behalf of the agency head in implementing and reviewing the agency's internal control program. This individual should have a broad knowledge of the agency's operations, personnel and policy objectives. Drawing on knowledge and experience with internal control matters, the internal control officer is a critical member of the management team who assists the agency head and other management officials by evaluating and improving the effectiveness of the internal control system. The Internal Control Officer is responsible for: establishing and maintaining a system of internal controls and program review; making management policies and guidelines available for all employees; and ensuring that employees have an adequate awareness and understanding of internal control standards through the implementation of education and training efforts. In general terms, the role of the Internal Control Officer is to work with appropriate personnel within the organization to coordinate the internal control activities and to ensure that the organization's internal control program meets requirements established by law and these standards.

While the Internal Control Officer has responsibility for reviewing the organization's internal control efforts and evaluating the adequacy of the internal control reviews, program and line managers are primarily responsible for conducting reviews to assure adherence to controls, and for analyzing and improving control systems. Ultimately, the organization's managers are still responsible for the appropriateness of the internal control system in their areas of operation.

The Internal Control Officer helps establish specific procedures and requirements; however, the effectiveness of these procedures and requirements must be audited by someone who was not involved in the process of putting them into place. The organization's internal auditor is responsible for evaluating the effectiveness of the system of internal control, and must be independent of the activities that are audited. For this reason, in nearly all instances, the internal auditor cannot properly perform the role of Internal Control Officer.

**Documentation of an Organization's Internal Control System**

Documentation is a necessary part of an effective internal control system. The level and nature of the documentation required will vary, based on the size of the entity and the complexity of the operational processes the entity performs. Management uses judgment in determining the extent of documentation that

is needed. Documentation is required for the effective design, implementation, and operating effectiveness of an entity's internal control system. These Standards includes minimum documentation requirements as follows:

- Management develops and maintains documentation of its internal control system.

- If management determines that a key internal control principle is not relevant, management supports that determination with documentation that includes the rationale of how, in the absence of that principle, the associated component could be designed, implemented, and operated effectively.

- Management documents in policies the internal control responsibilities of the organization.

- Management evaluates its operations and risks and documents its assessment of vulnerabilities.

- Management evaluates and documents the results of ongoing monitoring and separate evaluations to identify internal control issues.

- Management evaluates and documents internal control issues and determines appropriate corrective actions for internal control deficiencies on a timely basis.

- Management completes and documents corrective actions to remediate internal control deficiencies on a timely basis.

These requirements represent the minimum level of documentation of each component in an entity's internal control system. Management exercises judgment in determining what additional documentation may be necessary or an effective internal control system. If management identifies deficiencies in achieving these documentation requirements, the effect of the identified deficiencies is considered as part of management's summary determination as to whether the related principle is designed, implemented, and operating effectively.

**Part II: 5 Components and 17 Principles of Internal Control**

The 5 components of internal control must be successfully designed, implemented, and functioning sufficiently in order for the internal control system to be effective. The 17 principles represent the fundamental concepts which are associated with particular components within the system. All components and principles are relevant in establishing an effective internal control system. An organization that has a strong system of internal control exhibits the following actions.

| |
|---|
| **Control Environment**<br>**1. Demonstrates commitment to integrity and ethical values**<br>**2. Exercises oversight responsibility**<br>**3. Establishes structure, authority and responsibility**<br>**4. Demonstrates commitment to competence**<br>**5. Enforces accountability** |
| **Risk Assessment**<br>**6. Specifies suitable objectives**<br>**7. Identifies and analyzes risk**<br>**8. Assesses fraud risk**<br>**9. Manages risk during change** |
| **Control Activities**<br>**10. Selects and develops control activities**<br>**11. Selects and develops general controls over technology**<br>**12. Deploys controls through policies and procedures** |
| **Information and Communication**<br>**13. Uses relevant information**<br>**14. Communicates internally**<br>**15. Communicates externally** |
| **Monitoring**<br>**16. Conducts ongoing and/or separate evaluations**<br>**17. Evaluates and communicates deficiencies** |

**Control Environment**

Control environment encompasses the set of standards, processes, and structures that are the backbone for establishing internal control across the organization. It is the attitude toward internal control established and maintained by the management and employees of an organization. It is the product of management's governance—that is, its philosophy, style and supportive attitude—and the sense of competence, ethical values, integrity and morale. The control environment is further affected by the organization's structure and accountability relationships. The control environment has a pervasive influence on the decisions and activities of an organization, and provides the foundation for the overall system of internal control. If this foundation is not strong—if the control environment is not positive—the overall system of internal control will not be as effective as it should be.

The following principles describe how management is responsible for creating a positive control environment, and how employees are responsible for helping to maintain this environment.

**Demonstrates Commitment to Integrity and Ethical Values**

Integrity and ethical values are key elements contributing to a good control environment. In an organizational context, ethical values are the standards of behavior that form the framework for employee conduct, guiding employees when they make decisions. Management addresses the issue of ethical values when it encourages:

- honesty and fairness;
- recognition of and adherence to laws and policies;
- respect for the organization;
- leadership by example;
- commitment to excellence;
- appropriate respect for authority;
- respect for employees' rights; and
- conformance with professional standards.

Government employees should carry out their responsibilities with exemplary integrity, commensurate with their role as public servants. While it is management's responsibility to establish and communicate the values of the organization, it is everyone's responsibility to demonstrate integrity. Management encourages integrity by:

- establishing and publishing a code of conduct;
- complying with the organization's ethical values and code of conduct;
- rewarding employee commitment to the organization's ethical values;
- establishing methods for reporting ethical violations; and
- consistently enforcing disciplinary practices for all ethical violations.

**Exercises Oversight Responsibility**

*Governance*

Governance is the influence on an organization exercised by the executive body or the chief executive. The executive body may be a board of directors, board of trustees, council, legislature or similar entity. The chief executive may be the president, chancellor, commissioner, chief judge or an individual elected or appointed as the highest ranking person in the organization.

Their governance responsibilities are usually founded in a constitution, charter, laws, by-laws, regulations

and other similar documents. The leadership, actions and tone established and practiced by the governing body and/or executive can have a profound impact on how the employees of the organization perform their responsibilities, which in turn affects the achievement of the organization's mission.

Among the critical areas influenced by the governing body or executive are:

- approving and monitoring the organization's mission and strategic plan;
- establishing, practicing, and monitoring the organization's values and ethical code;
- overseeing the design, implementation, and operation of the organization's internal control system;
- providing direction to management on the correction of deficiencies in the internal control system;
- overseeing the decisions and actions of senior managers;
- establishing high-level policy and organizational structure;
- ensuring and providing accountability to stakeholders;
- establishing the overall management style, philosophy and tone; and
- directing management oversight of key business processes.

*Management's Operating Style and Philosophy*

Management's operating style and philosophy reflects management's basic beliefs regarding how the people and activities of an organization should be managed. There are many styles and philosophies. Although, some may be more effective than others in helping a particular organization accomplish its mission. Management should practice the most effective style and philosophy for the organization, making sure that its approach reflects the ethical values of the organization and positively affects staff morale. Management should practice and clearly communicate and demonstrate these beliefs to staff and periodically evaluate whether the style and philosophy are effective and are practiced consistently.

Management's philosophy and style can be demonstrated in such areas as: its approach to recognizing and responding to risks (both internal and external), including the potential for fraud; its acceptance of regulatory control imposed by others; its attitude toward internal and external reporting; its use of aggressive or conservative accounting principles; its attitude toward information technology and accounting functions; and its support for and responsiveness to internal and external audits and evaluations.

*Supportive Attitude*

A supportive attitude toward internal controls is a disposition that encourages desired outcomes. Since internal control provides management with reasonable assurance that the organization's mission is being accomplished, management should have a supportive attitude toward internal control and make sure that attitude permeates the organization. Executive management should set a tone that emphasizes the importance of internal control. Such a tone is characterized by:

- minimal and guarded use of control overrides;
- support for conducting control self-assessments and internal and external audits;
- openness and responsiveness to issues raised as the result of the evaluations and audits; and
- ongoing education to ensure everyone understands the system of internal control and their role in supporting it.

*Mission*

The mission of an organization should be formulated in a clear, concise statement, approved by executive management and/or the governing board of the organization. Management should tell employees about the organization's mission and explain how their jobs contribute to accomplishing the mission. The mission statement will be most effective if all employees perceive they have a personal stake in helping the organization fulfill its mission. Without a clearly defined and communicated mission, an organization may drift aimlessly and accomplish little.

As time passes, both internal and external changes can affect the organization's mission, goals and objectives. Therefore, management should periodically review the mission statement and update it, as necessary, for adequacy and relevancy.

*Morale*

Morale is the attitude people have about their work, as exhibited by their confidence, discipline and willingness to perform tasks. People's attitude about their jobs, work environment and organization affects how well they do their jobs. Management should recognize the importance of good morale in an effective control environment. Equally important, management should recognize that low employee morale can be detrimental to the control environment, causing a drop in productivity, turn over in key positions and lack of loyalty. Management should monitor the level of staff morale to ensure employees are committed to helping the organization accomplish its mission. Management should also take actions to maintain high morale. Such actions should provide staff with a sense that:

- their opinions and contributions are welcomed, valued and recognized;
- the organization is willing to help improve their level of competency;
- there is opportunity for continuous improvement;
- they have a stake in the mission, goals and objectives of the organization;
- the organization's appraisal and reward systems are fair and consistent;
- disciplinary actions are fair, consistently applied and timely; and
- the lines of communication are open.

**Establishes Structure, Authority and Responsibility**

Structure is the framework in which the organization's plans are carried out. It should define the functional subunits of an organization and the relationships among them.

An organizational chart can provide a clear picture of the authority and accountability relationships among

functions. The chart should be provided to all employees to help them understand the organization as a whole, the relationships among its various components and where they fit into the organization. Management should review this chart periodically to ensure it accurately reflects the organization's structure.

Management should delegate authority and responsibility throughout the organization. Management is responsible for organizing the entity's authority and accountability relationships among various functions to provide reasonable assurance that work activities are aligned with organizational objectives. With increased delegation of authority and responsibility, there is a need to provide qualified and continuous supervision and to monitor results. Supervision throughout the organization helps ensure that employees are aware of their duties and responsibilities, and know the extent to which they are accountable for the successful completion of specific activities.

**Demonstrates Commitment to Competence**

Competent employees have the skill, knowledge and ability to perform their assigned tasks. Management's responsibility for ensuring the competency of its employees should begin with establishing appropriate human resource policies and practices that reflect a commitment to:

- establishing levels of knowledge and skill required for every position;
- verifying the qualifications of job candidates;
- hiring and promoting only those with the required knowledge and skills;
- establishing training and education programs that help employees increase their knowledge and skills;
- planning and preparing for succession by developing contingency plans for the assignment of responsibilities when employees change positions or leave the organization.

Management should also ensure that employees have adequate resources, such as equipment, software, policy and procedure manuals, as well as the tools and support they need to perform their jobs.

**Enforces Accountability**

Management should evaluate performance and hold individuals accountable for their responsibilities in pursuit of organizational objectives. Accountability is driven by the tone at the top and supported by the commitment to integrity and ethical values. Management holds individuals accountable through mechanisms such as performance evaluations and disciplinary actions. Actions to enforce accountability for organizational responsibilities range from information feedback provided by the direct supervisor to formal disciplinary action. The level of enforcement action is determined by the significance of the deficiency to the internal control system.

Management is responsible for evaluating the pressure exerted on individuals to fulfill their assigned duties. Excessive pressure can result in individuals skipping steps or cutting corners to meet established goals. Management can adjust excessive pressures by rebalancing workloads or increasing resource levels.

**Risk Assessment**

Risk is the possibility that an event will occur and threaten or otherwise adversely affect the achievement of the organizations objectives. Objectives can only be derived from and must be in alignment with the organization's mission, strategic plan, and performance goals. Management should define objectives clearly to enable the identification of risks and define risk tolerances. The act of managing the risks associated with achieving an origination's mission through its objectives requires an assessment of these risks.

Risk assessment involves a dynamic and iterative process for identifying and analyzing these threats through an organization-wide effort, forming a basis for determining how risks should be managed. Management considers possible changes in the external environment and within its own business model that may impede its ability to achieve its objectives. For each risk that is identified, management should decide whether to accept the risk, reduce the risk to an acceptable level, or avoid the risk. Risk management is an ongoing process that must include monitoring the changing environment and tracking planned actions to mitigate the impact and likelihood of risks.

**Specifies Suitable Objectives**

Objectives are driven by an organization's mission and its strategic plan, which outlines goals and priorities. Objectives detail an organization's areas of focus for accomplishing its mission and meeting its expectations. Management sets internal expectations and requirements through the established standards of conduct, oversight structure, organizational structure, and expectations of competence. Management should evaluate whether defined objectives are consistent with these requirements and expectations, and make revisions as necessary. This consistency enables management to identify and analyze risks associated with achieving the defined objectives as part of the control environment.

By stating objectives in specific and measurable terms, the design of internal control for related risks can be better understood at all levels of the organization. This involves clearly defining what is to be achieved, who is to achieve it, how it will be achieved, and the time frames for achievement. Measurable objectives are generally free of bias and do not require subjective judgment. Measurable objectives are also stated in a quantitative or qualitative form that permits reasonably consistent assessment. For quantitative objectives, performance measures may be a targeted percentage or numerical value. For qualitative objectives, management may need to design performance measures that indicate a level or degree of performance, such as milestones.

Risk tolerance is the acceptable level of variation in performance relative to the achievement of objectives. Management defines the risk tolerances for defined objectives by ensuring that the set levels of variation for performance measures are appropriate for the design of an internal control system. Risk tolerances should be measured in similar terms as the performance measures for instance, if accuracy is a measure of an objective, then risk tolerance would be stated as an acceptable error rate, note that the concept of risk tolerance does not apply to compliance, since an entity is either compliant or not compliant.

Further, management must consider the risk tolerances in the context of the entity's applicable laws, regulations, and standards as well as the entity's standards of conduct, oversight structure, organizational structure, and expectations of competence. If risk tolerances for defined objectives are not consistent with these requirements and expectations, management must make appropriate revisions to achieve consistency.

**Identifies and Analyzes Risk**

One of the most important components of an organization's internal control program is the process used to identify and evaluate the risks and internal controls associated with specific functions, objectives, and

assessable units.

*Identify Risk*

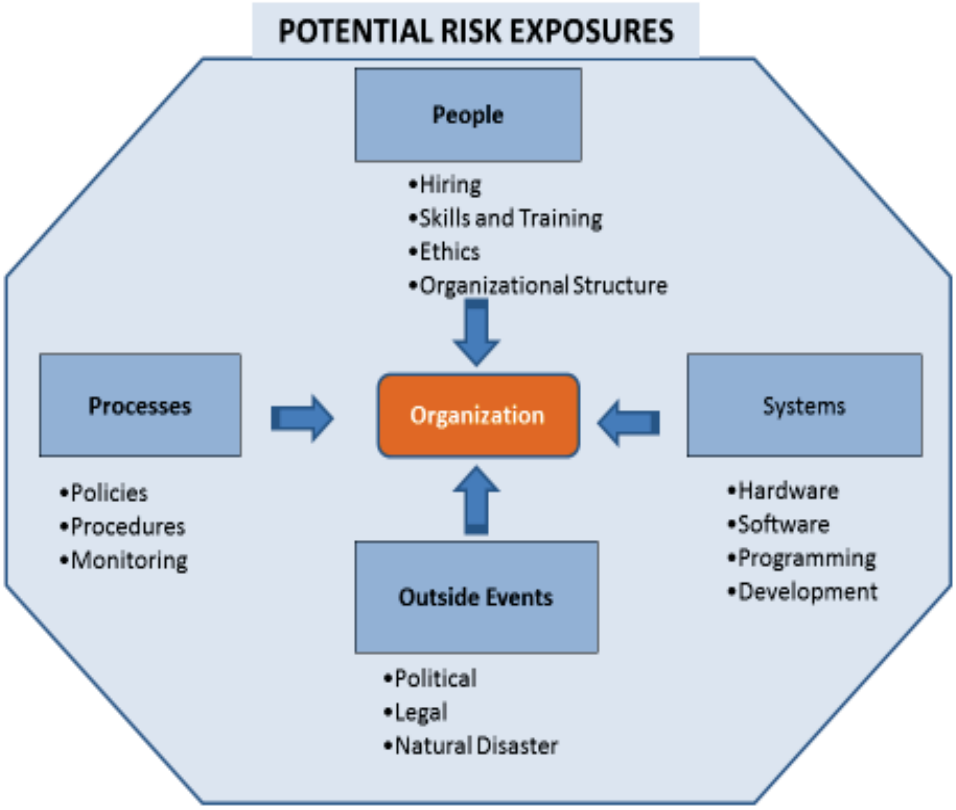
Management first needs to identify all business objectives of its programs and units, including operational goals, reporting, and compliance requirements. These objectives should be specific enough to provide direction for managing the organization's functions and should be stated in terms that reflect the responsibilities of its subunits. Business objectives should flow from the three objectives of internal control, which were discussed in Part I. For example, the following two business objectives are derived from the operational objective of internal control:

- Ensure all applications are processed (i.e., promoting the effectiveness and efficiency of the entity's operation).

- Ensure access to electronic files is restricted to authorized personnel (i.e., safeguarding assets against loss).

After identifying all the business objectives, managers should identify all the risks associated with each objective (i.e., the events that would threaten the accomplishment of each objective). These risks can be both internal (e.g., human error, fraud, system breakdowns) and external (e.g., changes in legislation, natural disasters). It is essential that managers within the organization identify the risks associated with their respective objectives. There are many ways to look at risks, and no one can identify all potential risks. One recognized approach is to conduct a group brainstorming session with staff to generate ideas on what could go wrong in an organization, operation, or unit. It's a dynamic process, allowing you to consider how potential events might affect the achievement of your objectives.

The following chart illustrates some of the places where an organization can be exposed to risk, although it is not reflective of all potential risks.




The Appendix includes references to many other resources that can help management select the most effective tools and approaches for its operations.

*Information Technology Risk*

As organizations continue to develop or incorporate technological advances, they become exposed to new and sometimes greater risks. Therefore, organizations must identify and assess the risks accompanying each new device, platform, software application or business model. Among the questions management should consider are:

- How does the new technology contribute to achieving the organization's mission?
- Does the new technology increase risks that may hinder the accomplishment of objectives?
- Examples may include reduced data security, frequent or prolonged service interruptions, steep learning curves, or decreased morale.
- What changes to internal controls (e.g., control activities) are necessary to manage these risks?

Interdependencies among risks often cross business unit and functional boundaries. In recent years, government organizations have increasingly turned to third-party service providers for information technology solutions. Organizations use third parties for a variety of purposes, ranging from simple web

hosting to complete outsourcing of all information technology (IT) functions. Outsourcing provides organizations with a number of benefits including the ability to utilize technology that may not otherwise be available, to access other skills and knowledge that may not exist in the organization, or to provide 24 hour-a-day, seven-day-a-week support.

The impact that third parties have on an organization can vary considerably. Third parties that provide little more than connectivity services, may have little impact on an organization's internal controls and related control objectives. Conversely, third parties that provide services ranging from application hosting to business process outsourcing to complete management of all IT-related functions can have significant impact on an organization's internal controls and related control objectives.

Regardless of the level of impact a third party can have on an organization, the governing board or organizational head and senior management are ultimately responsible for managing activities conducted through third-party relationships as well as identifying and controlling the risks arising from such relationships to the same extent as if the activity were handled within the organization. Third-party activities must be included in the organization's risk assessment, and management should implement an effective third party risk management process. Management should appropriately assess, measure, monitor, and control the risk associated with the third-party relationship. Organizations can choose to perform these assurance activities on their own or require an independent assessment of the controls around the services provided. In either situation, the organization should provide for these assurances in the agreement (contract) with the third-party and clearly state its expectations including compliance with these Standards. Management should consider designating a specific officer to coordinate the oversight activities and involve other operational areas in the monitoring process. An effective oversight program will generally include the monitoring of the third party's quality of service, risk management practices, and applicable internal controls.

In some instances in government operations, a third party may be another governmental entity. In those situations, wherever possible, establishing a Memorandum of Understanding (MOU) will help to clarify the requirements for both entities. Agreement on which processes each organization is responsible for, how assurances will be provided and in what format are all factors to include in such an agreement. Where an MOU does not exist, the risks associated with the outsourcing should still be recorded and tracked on a continuous basis. While it may be difficult to fully mitigate risks associated with such arrangements, it is important to inventory these risk and monitor for their occurrence with a plan for response in place should they occur.

*Analyze Risk*

Management should evaluate each identified risk in terms of its impact and its likelihood of occurrence, as follows:

- Impact is the effect an unfavorable event would have on the organization. This effect could be some type of harm or an opportunity that would be lost. The impact is also affected by how quickly an event may happen or spread (speed) and its duration. If possible, these impacts should be quantified or, at the very least, should be described in terms that are specific enough to indicate the significance of the risk.

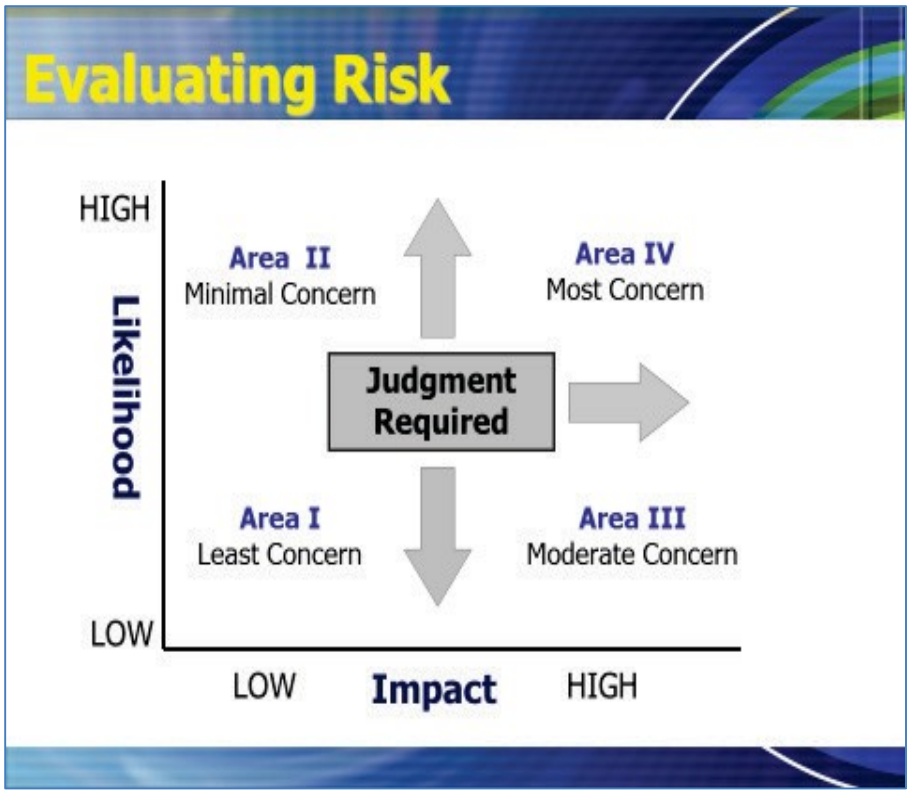
- Likelihood of occurrence is the probability that an unfavorable event would occur if there were no control activities (as described in the following section) to prevent or reduce the risk. A likelihood of occurrence should be estimated for each identified risk.

The combination of the two factors provides management with a rating for each risk identified. Further, management should identify the amount of risk they are willing to accept in relation to achieving objectives; thereby effectively quantifying management's tolerance for such risks.

Management should use judgment to establish priorities for risks based on their impact and their likelihood of occurrence. Risks should be ranked in a logical manner, from those that are most significant (high impact) and most likely to occur (high likelihood) to the least significant (low impact) and least likely (low likelihood).

This chart depicts one reasonable approach that management may choose to employ to evaluating risks, where Area 1 represents the lowest priority risk and Area 4 represents the highest.

For example, a program manager may have control over two cash accounts: one, the office petty cash fund and the other, for collection of fees and fines from a program activity. Most people would likely consider the petty cash fund to be an Area 1 or 2 risk based on its small balance. In contrast, if management finds that the fees and fines are substantial in amount, are stored in an unlocked location and that there is a six-month backlog in processing them, this would likely result in an Area 4 assessment requiring immediate attention.




Risks may be analyzed on an individual basis or grouped into categories with related risks and analyzed collectively. Regardless of whether risks are analyzed individually or collectively, management should consider the correlation among different risks or groups of risks when estimating their significance. The specific risk analysis methodology used can vary by entity because of differences in missions and the difficulties inherent in qualitatively and quantitatively defining risk tolerances.

*Respond to and Manage Risk*

Executive management should provide guidance to managers throughout the organization to help them assess both the level and the nature of risks that and distinguish acceptable from unacceptable risks. Managers should use this guidance, along with the results of the organization's specific risk assessments, to determine actions necessary to manage each risk to an acceptable level. In each case, managers must decide whether to accept, reduce, transfer or avoid each risk entirely.

For example, in deciding how to manage the risk that unauthorized persons could gain access to electronic files, managers should consider the following possibilities:

- Accept the risk: Do not establish control activities - Management may choose to accept the risk of unauthorized access because it determines that the consequences of such access are not significant. (E.g., the files may not contain data that is sensitive.) Management might also choose to accept the risk if the cost of the associated control activities is greater than the cost of the unfavorable event.

- Reduce the risk: Establish control activities - Management cannot accept the current level of risk of unauthorized access because the files contain confidential or otherwise inherently valuable data. Therefore, management establishes control activities that are intended to reduce the risk of unauthorized access to an acceptable level. However, the risk is reduced only as long as the control activities function as intended.

- Transfer or share the risk - Management may decide to maintain electronic data in a vendor-operated cloud environment or an external data center operated by a business partner. Contract provisions may then allow management to transfer responsibility for all or part of the risk of improper access to the service provider or business partner.

- Avoid the risk: Do not carry out the function - Management determines that it cannot tolerate any risk of unauthorized access to the files or cannot adequately control such access. For example, a file may contain extremely sensitive data, or access controls may not be feasible. In this case, management may decide that the impact of any unauthorized access to this file would be too risky or that access is too difficult or too costly to control. Therefore, management decides not to carry out this function (i.e., decides not to maintain the data).

*Reduce Risk*

In most cases, government entities do not have the ability to eliminate programs to wholly avoid risks, and options to share or transfer risks to others are also limited. As a result, management must most often take actions to reduce risks to acceptable levels. Management should therefore use risk assessment information to help identify the most effective and efficient control activities available for handling the risk. Specifically, management should answer the following questions:

- What is the cause of the risk? Consider the reasons the risk exists to help identify all the possible control activities that could prevent or reduce the risk.

- What is the potential for fraud? Consider potential threats that could result in fraudulent activities.

- What is the cost of control vs. the cost of the unfavorable event? Compare the cost of the risk's impact with the cost of carrying out various control activities, and select the most cost- effective choice.

- What is the priority of this risk? Use the prioritized list of risks to help decide how to allocate resources among the various control activities used to reduce the risks. The higher the priority, the greater the resources which may be allocated to the control activities intended to reduce the risk.

Management should maintain its analysis and interpretation of the risk assessment information as part of its documentation of the rationale that supports its risk management decisions. Management should review these decisions periodically to determine whether changes in conditions warrant a different approach to managing and reducing risk.

**Fraud Risk**

All organizations need to consider the potential for fraud to occur in their operations. Fraud is any intentional act or omission designed to deceive others, resulting in the victim suffering a loss and/or the perpetrator achieving a gain. Occupational fraud is the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets.

Fraud should be included as part of the risk assessment process, but can be documented separately or in conjunction with other risks. The organization should consider and assess the following when evaluating potential risks for fraud:

- Various Types of Fraud - fraudulent reporting, possible loss of assets, and corruption resulting from the many ways that fraud and misconduct can occur.

- Incentives and Pressures - internal and external motives and demands.

- Opportunities - vulnerabilities to unauthorized acquisition, use, or disposal of assets, altering of the entity's reporting records, or other inappropriate acts. Also consider the opportunities for fraud and abuse afforded certain positions or scopes of authority over operations.

- Attitudes and Rationalizations - how management and other personnel might engage in or justify inappropriate actions.

Management analyzes and responds to identified fraud risks so that they are effectively mitigated. As part of analyzing fraud risk, management also assesses the risk of management override of controls. Management responds to fraud risks through the same risk response process performed for all analyzed risks. Management designs an overall risk response and specific actions for responding to fraud risks. It may be possible to reduce or eliminate certain fraud risks by making changes to the entity's activities and processes. These changes may include stopping or reorganizing certain operations and reallocating roles among personnel to enhance segregation of duties. In addition to responding to fraud risks, management may need to develop further responses to address the risk of management override of controls.

Further, when fraud has been detected, the risk assessment process may need to be revised. In addition to fraud, management considers other forms of misconduct that can occur, such as waste and abuse. Waste is the act of using or expending resources carelessly, extravagantly, or to no purpose. Abuse involves behavior that is deficient or improper when compared with behavior that a prudent person would consider reasonable and necessary operational practice given the facts and circumstances. This includes the misuse of authority or position for personal gain or for the benefit of another. Waste and abuse do not necessarily involve fraud or illegal acts.

**Manages Risk During Change**

When change occurs in an organization, it often affects the control activities that were designed to prevent or reduce risk. Some examples of change include: new processes, new systems, significant changes in job responsibilities, reorganizations, significant changes in personnel, and changes in legislation. To properly manage risk, management should:

- monitor changes to ensure that each risk continues to be managed as change occurs;

- inform employees responsible for managing the organization's most critical risks about any

proposed changes that may affect their ability to manage those risks; and

- continually monitor the factors that can affect the risks already identified as well as other factors that could create new risks.

**Control Activities**

Control activities are the actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out. Management should establish control activities that are effective and efficient and contribute to the mitigation of risks.

**Selects and Develops Control Activities**

When designing and implementing control activities, management should strive for the maximum benefit at the lowest possible cost. Here are a few simple rules to follow:

- The cost of the control activity should not exceed the cost that would be incurred by the organization if the undesirable event occurred.

- Management should build control activities into business processes and systems as the processes and systems are being designed. Adding control activities after the development of a process or system is generally more costly.

- The allocation of resources among control activities should be based on the impact and likelihood of the risk they are intended to reduce.

Control activities may include a variety of approaches to mitigate risks, considering both manual and automated as well as preventive and detective controls.

- Preventive controls are designed to deter the occurrence of an undesirable event. The development of these controls involves anticipating potential problems before they occur and implementing ways to avoid them.

- Detective controls are designed to identify undesirable events that do occur, and alert managers so they can take corrective action promptly.

Preventive controls can often be more expensive to operate and maintain than detective controls. Costs and benefits should be assessed before control activities are implemented. Management should also remember that an excessive use of preventive controls can impede productivity. No one control activity provides all of the answers to risk management problems. In some situations, a combination of control activities should be used, and in others, one control activity could substitute for another. The following are descriptions of some of the more commonly used control activities. This is by no means an exhaustive listing of the alternatives available to management.

*Documentation*

Documentation involves preserving evidence to substantiate a decision, event, transaction or system. All documentation should be complete, accurate and recorded timely. Documentation should have a clear purpose and be in a usable format that will add to the efficiency and effectiveness of the organization. Examples of areas where documentation is important include critical decisions, significant events,

transactions, policies, procedures and the system of internal control.

Critical decisions and significant events usually involve executive management. These decisions and events usually result in the use, commitment, exchange or transfer of resources, such as in strategic plans, budgets and executive policies. By recording the information related to such events, management creates an organizational history that can serve as justification for subsequent actions and decisions and will be of value during self-evaluations and audits.

Documentation of transactions should enable managers to trace each transaction from its inception through its completion. This means the entire life cycle of the transaction should be recorded, including: (1) its initiation and authorization; (2) its progress through all stages of processing; and (3) its final classification in summary records. For example, the documentation for the purchase of equipment would start with the authorized purchase request and continue with the purchase order, the vendor invoice and the final payment documentation.

Documentation of policies and procedures is critical to the daily operations of an organization. The organization deploys control activities through policies that establish what is expected and through procedures that put policies into action. These documents set forth the fundamental framework and the underlying methods and processes all employees rely on to do their jobs. They provide specific direction to employees in their daily decision making. Without this framework of understanding by employees, conflict can occur and poor decisions can be made, causing serious harm to the organization's reputation. Further, the efficiency and effectiveness of operations can be adversely affected.

The documentation of an organization's system of internal control should include the organization's structure, policies, assessable units, control objectives and control activities. The various aspects of a system of internal control can be represented in narrative form, such as in policy and procedure manuals, and/or in the form of flow charts or matrices.

*Approval and Authorization*

Approval is the confirmation or sanction of employee decisions, events or transactions based on a review. Management should determine which items require approval based on the level of risk to the organization without such approval. Management should clearly document its approval requirements and ensure that employees obtain approvals in all situations where management has decided they are necessary. For example, a manager reviews a purchase request from an employee to determine whether the item is needed. Upon determining the need for the item, the manager signs the request; indicating approval of the purchase.

Authorization is the power management grants employees to carry out certain duties, based on approval received from supervisors. Authorization is a control activity designed to ensure events or transactions are initiated and executed by those designated by management. Management should ensure that the conditions and terms of authorizations are clearly documented and communicated, and that significant transactions are approved and executed only by persons acting within the scope of their authority. For example, a manager may be authorized by his or her supervisors to approve purchase requests, but only those up to a specified dollar amount.

*Verification*

Verification is the determination of the completeness, accuracy, authenticity and/or validity of transactions, events or information. It is a control activity that enables management to ensure activities are being done in accordance with directives. Management should determine what needs to be verified, based on the risk to the organization if there were no verification. Management should clearly communicate and document

these decisions to those responsible for conducting the verifications. An example of verification is ensuring that a fair price has been obtained in a purchase and funds are available to pay for the purchase.

*Supervision*

Supervision is the ongoing oversight, management and guidance of an activity by designated employees to help ensure the results of the activity achieve the established objectives. Those with the responsibility for supervision should:

- monitor, review and approve, as appropriate, the work of those performing the activity to ensure the work is performed correctly;
- provide the necessary guidance and training to help minimize errors and waste and to ensure that employees understand and follow management directives; and
- clearly communicate the duties and responsibilities assigned to those performing the activities.

An example of supervision is when an assigned employee (supervisor) reviews the work of another employee processing a purchase order to determine whether it is prepared accurately and completely and has been properly authorized. The supervisor then signs the order to signify his or her review and approval. However, if there are any errors, the supervisor would return the order to the employee and explain how to complete the request properly.

*Separation of Duties*

Separation of duties is the division of key tasks and responsibilities among various employees and subunits of an organization. By separating key tasks and responsibilities - such as receiving, recording, depositing, securing and reconciling assets - management can reduce the risk of error, waste, or wrongful acts. The purchasing cycle is an area where the separation of duties can minimize the risk of inappropriate, unauthorized or fraudulent activities. Specifically, the various activities related to a purchase (initiation, authorization, approval, ordering, receipt, payment and record keeping) should be done by different employees or subunits of an organization. In cases where tasks cannot be effectively separated, management can substitute increased supervision as an alternative control activity that can help prevent or reduce these risks.

*Safeguarding Assets*

The safeguarding of assets involves restricting access to resources and information to help reduce the risk of unauthorized use or loss. Management should protect the organization's equipment, information, documents and other resources that could be wrongfully used, damaged or stolen. Management can protect these resources by limiting access to authorized individuals only. Access can be limited by various means such as locks, passwords, electronic firewalls and encryption. Management should decide which resources should be safeguarded and to what extent. Management should make this decision based on the vulnerability of the items being secured and the likelihood of loss.

*Reporting*

Reporting is a means of conveying information. It serves as a control when it provides information on issues such as timely achievement of goals, budget status and employee concerns. Reporting also helps to promote accountability for actions and decisions. An example of a report that serves as a control activity would be one that compares purchasing activities with the approved budget, indicating and explaining significant variances between the two.

**Control Activities for Information Technology**

While some of the control activities relating to information technology (IT) are the responsibility of specialized IT personnel, other IT control activities are the responsibility of all employees who use computers in their work. For example, any employee may use:

- encryption tools, protocols, or similar features of software applications that protect confidential or sensitive information from unauthorized individuals;
- backup and restore features of software applications that reduce the risk of lost data;
- virus protection software; and
- passwords that restrict user access to networks, data and applications.

IT control activities can be categorized as either general or application controls. General controls apply to all computerized information systems, including mainframes, personal computers, server networks, virtual private networks and end-user environments. Application controls apply to the processing of data within the application software.

General and application controls are interrelated. General controls support the functioning of application controls, and both types of controls are needed to ensure complete and accurate information processing.

*General Controls*

General controls are concentrated on six major types of control activities: an entity-wide security management program; access controls; application software development and change; system software controls; segregation of duties; and service continuity.

- An organization-wide security management program includes a comprehensive, high-level assessment of risks to information systems. An organization should have a plan that clearly describes its security management program and policies and the procedures that support it, including procedures for the secure storage and disposal of sensitive information. The organization should also establish a structure to implement and manage the security program with security responsibilities clearly defined. In addition, the organization should monitor the effectiveness of the security program and make changes as needed.
- Access security controls are physical and software processes to prevent or detect unauthorized access to systems and data. These controls protect the systems from inappropriate access and unauthorized use by hackers and other trespassers, and form inappropriate use by agency personnel. Specific control activities may include:
    - restrictions on users allowing access only to the system functions they need to perform their assigned duties;
    - software and hardware firewalls to restrict access to assets, computers, and networks by external persons; and

- frequent changes of passwords and deactivation of former employees' passwords.

- Application software development and change control provides the structure for the safe development of new systems and the modification of existing systems. Control activities should include: system documentation requirements; authorizations for undertaking projects; and reviewing, testing, and approving development and modification activities before placing systems into operation.

- System software control is the controlling and monitoring of access to use and changes made to system software, including: security procedures over the acquisition, implementation, and maintenance of all system software; data-based management systems; telecommunications; security software; and utility programs.

- The concept of segregation of duties in a computer environment is the same as in a manual process. Key tasks and responsibilities should be divided among various employees and subunits of the computer operations. No one individual should control all of the primary elements of a transaction, event or process. Identifying incompatible duties and implementing policies to separate those duties can be monitored through the use of access controls as well as by implementing operating procedures, supervision, and the review of employee activities.

- Service continuity is concerned with maintaining or re-establishing the activities or level of service provided by an organization in the event of a disaster or other damaging occurrence. It is critical that an organization have backup and recovery procedures, and contingency and disaster plans. Data center and client-server operation controls involve steps to prevent and minimize potential damage to hardware and software and the interruption of service through the use of data and program backup procedures. Such procedures include: off-site storage of backup data; environmental controls; staff training; and hardware maintenance and management. Organizations should develop, document and periodically test their contingency plans.

*Application Controls*

Application controls help ensure that transactions are valid, properly authorized, and processed and reported completely and accurately. These controls also take into account the whole sequence of transaction processing, from the preparation of the initial source document or online data entry to the creation and use of the final output. As such, application controls consist of input, processing, and output controls:

- Input controls include processes for verifying data accuracy and completeness upon data entry to a system. These controls also provide specific mechanisms for input authorization, data conversion, data editing and error handling.

- Processing controls help ensure that data remains complete and accurate during updating, and that the application programs perform as intended.

- Output controls help ensure that system-generated information is accurate, properly recorded, and received or reviewed by authorized individuals only.

As information technologies advance and Internet use increases, modifications will have to be made in each organization's specific IT control activities. However, the basic requirements of control will not change. As more powerful computers place more responsibility for data processing in the hands of the end users and as Internet use grows, organizations must be prepared to implement the controls necessary to maintain an effective system of internal control.

This information is not meant to be a complete explanation of all IT control activities. Additional guidance has been issued by the New York Office of Information Technology Services. Further guidance can also be obtained from sources such as ISACA's COBIT 5: A Business Framework for the Governance and Management of Enterprise IT and the National Institute of Standards and Technology's special publications.

**Deploys Controls Through Policies and Procedures**

Management documents, in policies, the internal control responsibilities of the organization. This documentation generally consists of the following:

- each unit's responsibility for an operation process's objectives and related risks;
- control activity design;
- implementation; and
- operating effectiveness.

Individuals in key internal control roles may further define policies for day-to-day procedures depending on the propensity for change in the environment and the complexity of the process. Policies should be communicated and available to employees in accordance with their duties, and management should ensure employees understand their responsibilities related to policies affecting their functions. Further, management should periodically and systematically review policies, procedures and related control activities for relevance and effectiveness in achieving objectives and addressing related risks.

**Information and Communication**

Information is necessary for the organization to carry out internal control responsibilities to support the achievement of its objectives. Management obtains or generates and uses relevant and high quality information from both internal and external sources, as well as providing communication internally and externally to support the functioning of other components of internal control.

**Uses Relevant Information**

Management uses relevant and high quality information to make informed decisions and evaluate the organization's performance in achieving key objectives and addressing risks. For information to be relevant, it must come from reliable internal and external sources in a timely manner based on the identified information requirements. Quality information must be appropriate, current, complete, accurate, accessible, and provided on a timely basis.

**Communicates Internally**

Internal communication is the continual, iterative process of obtaining, providing, and sharing necessary information. Information should be communicated to management and other employees who need it in a form and within a time frame that helps them to carry out their responsibilities. It enables personnel to receive a clear message from senior management that control responsibilities must be taken seriously.

Information can be communicated verbally, in writing and electronically. While verbal communication may be sufficient for many day-to-day activities, it is best to document important information. This provides a more permanent record and enables managers and others to review the information.

Information should travel in all directions (across, up and down an organization) to ensure that all members of the organization are informed and that decisions and actions of different units are communicated and coordinated. A good system of communication is essential for an organization to maintain an effective system of internal control. A communication system consists of methods and records established to identify, capture and exchange useful information. Information is only useful when it is timely, sufficiently detailed and appropriate to the user.

Management should establish communication channels that:

- provide timely information;
- can be tailored to individual needs;
- inform employees of their duties and responsibilities;
- enable the reporting of sensitive matters;
- enable employees to provide suggestions for improvement;
- provide the information necessary for all employees to carry out their responsibilities effectively; and
- convey top management's message that internal control responsibilities are important and should be taken seriously.

Internal communication is not an isolated internal control component. It affects every aspect of an organization's operations and helps support its system of internal control. All aspects of a strong internal control system are reliant on timely, relevant and accurate communication methods. An organization must internally communicate information, including objectives and responsibilities for internal control, to support the functioning of all other components of the internal control system. Further, feedback from this communication network can help management evaluate how well the various components of the system of internal control are working.

**Communicates Externally**

External communication with customers, suppliers, regulators and other outside parties is also essential to effective internal control. Information should be communicated externally through appropriate reporting lines so that external parties can help the entity achieve its objectives and address related risks.

Management should establish separate reporting lines that:

- allow for whistleblower and ethics hotlines for communicating confidential information;
- inform external parties of these separate reporting lines;
- educate the public and employees as to how these reporting lines operate;
- convey how these reporting lines are to be used; and
- instruct how the information will remain confidential.

External information can also be communicated verbally, in writing and electronically. Management considers a variety of factors when selecting an appropriate method of communication including its audience, nature of information provided, availability, cost, and legal or regulatory requirements.

**MONITORING**

**Conducts Ongoing and/or Separate Evaluations**

Monitoring is the ongoing evaluation of internal control components, either individually or as a whole system, to ascertain whether they are present and functioning. Management should focus monitoring efforts on internal control and achievement of the organization's mission.

Everyone within an organization has some responsibility for monitoring. The position a person holds in the organization helps to determine the focus and extent of these responsibilities. Therefore, the monitoring performed by staff, supervisors, mid-level managers and executives will not have the same focus, as follows:

- **Staff** - The primary focus of staff members should be on monitoring their own work to ensure it is being done properly. They should correct the errors they identify before work is referred to higher levels for review. Management should educate staff regarding control activities and encourage them to be alert to and report any irregularities. Because of their involvement with the details of the organization's daily operations, staff members have the best vantage point for detecting any problems with existing control activities. Management should also remind staff to note changes in their immediate internal and external environments, to identify any risks and to report opportunities for improvement.

- **Supervisors** - Supervision is a key element of monitoring. Supervisors should monitor all 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.

- **Mid-Level Managers** - Mid-level managers should assess how well controls are functioning in multiple units within an organization, and how well supervisors are monitoring their respective units. The focus of these managers should be similar to that of supervisors, but should extend to cover all the units for which they are responsible.

- **Executive Management** - Executive management should focus their monitoring activities

on the major divisions of the organization. Because of this broader focus, executive managers should place even more emphasis on monitoring the achievement of the organization's goals. Executive managers should also monitor for the existence of risks and opportunities in either the internal or external environment that might indicate the need for a change in the organization's plans.

Management should ensure that it takes the proper actions to address the results of monitoring. For example, management may decide to establish new goals and objectives to take advantage of newly identified opportunities, may counsel and retrain staff to correct procedural errors or may adjust control activities to minimize risk in response to changed circumstances. Further, independent evaluations should be performed periodically to provide objective feedback.

The monitoring performed by staff, supervisors, mid-level managers and executives should focus on the following major areas:

- Control Activities - Control activities are established to prevent or reduce the risk of an unfavorable event from occurring. If these activities fail, the organization becomes exposed to risk. Control activities can fail when controls are overridden, or when there is collusion for fraudulent purposes. Therefore, management should establish procedures to monitor the functioning of control activities and the use of control overrides. Management should also be alert to signs of collusion. Effective monitoring gives management the opportunity to correct any control activity problems and to control the risk before an unfavorable event occurs.

- Mission - Monitoring activities should include the development and review of operational data that would allow management to determine whether the organization is fulfilling its mission. This can be achieved by periodic comparison of operational data to the organization’s strategic plan.

- Control Environment - Executive management should monitor the control environment to ensure that managers at all levels are maintaining established ethical standards of behavior and that staff morale is at an appropriate level. Managers should also ensure that the staff is competent, that training is sufficient and that management style and philosophy foster the accomplishment of the organization's mission.

- Information and Communication - Managers should periodically verify that the

- employees they are responsible for are receiving and sharing information appropriately, and that this information is timely, sufficient and appropriate for the users. Management should ensure that there are open lines of communication, which fosters reporting of both positive and negative results.

- Risks and Opportunities - Managers should also monitor the organization's internal and external environment to identify any changes in risks and the development of opportunities for improvement. If changes are identified, managers should take appropriate action to address these new or changed risks and opportunities. Management should recognize that delays in responding to risks could result in damage to the organization, and a missed opportunity may result in a loss of new revenue or savings.

**Evaluates and Communicates Deficiencies**

Management must evaluate and communicate 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. For monitoring to be most effective, all employees need to understand the organization's mission, objectives, and risk tolerance levels as well as their own responsibilities. (See Part III for further details on evaluation).

## Part III: Managing and Evaluating the Internal Control System

These Standards are not intended to dictate a specific structure for managing and evaluating a system of internal control in New York State government operations. That being said, there are common attributes present among operations that have strong systems of internal control. This section highlights the elements common to successful systems of internal control.

### Responsibility for Managing the System

This may come as a surprise to some readers, but external and internal auditors are not responsible for an entity's internal controls. External auditors evaluate internal controls as part of their audit planning process to determine if they can be relied on for purposes of issuing financial statements. Internal auditors assess whether an organization's internal controls are effective and evaluate the way an organization operates. Neither is responsible for the design and effectiveness of controls. An organization's management (including any applicable governing board) is responsible for making sure that the right controls are in place, and that they are performing as intended.

If an entity has a governing board, that board's responsibilities for internal controls primarily involve oversight, authorization and ethical leadership. If an entity does not have a governing board, this overarching responsibility falls to the head of the organization (e.g., Commissioner, Executive Director). Generally, governing boards or organizational heads do not design internal controls or prepare the written policies they adopt. Instead, the governing board relies upon management, especially the executive operational head (e.g., Executive Deputy, Deputy Director), to create the policies needed to ensure that the organization accomplishes its mission. Executive management in turn relies upon managers and department heads to recommend and implement procedures that lower identified risks. Wherever the responsibility for final approval of policies and procedures lies, this group or individual should take great care in reviewing these directives to ensure they are addressing risk appropriately.

Within the managerial ranks, the executive operational head provides the leadership needed to establish and guide an integrated internal control framework. This individual must establish a positive "tone at the top" by conducting the organization's affairs in an honest and ethical manner and by establishing accountability at all levels of the organization. If the executive operational head does not demonstrate strong support for internal controls, the organization as a whole will be unlikely to practice good internal controls.

While the executive operational head is responsible for the design and maintenance of the entity's control framework, the operational managers and department heads are the front line for implementing and monitoring internal controls. These individuals are responsible for supporting the internal control initiatives of the board and/or organizational and operational heads of the organization in daily operations. All levels of management must work together to create an integrated framework that lowers risk to an acceptable level and assists the organization in meeting its goals and objectives. Managers and department heads are generally responsible for identifying potential risks, designing and implementing controls for their areas of responsibility, and keeping current with events and changes that may affect the controls they have put into place.

### The Importance of Internal Control and Risk Management

For New York State government operations, compliance with the spirit of the Internal Control Act will go a long way toward realizing the benefits of effective internal control and risk management. Compliance is best accomplished by having a system of internal control whose principal aim is to manage risks that

threaten the achievement of an organization's objectives. This entails not only performing risk assessments as discussed in the previous section of these Standards, but also:

- Identifying the organization's risk tolerance (e.g., margin of error, materiality) and what is deemed an unacceptable event;

- Monitoring legislation, market conditions, or political changes and their resulting potential impact on the organization on an ongoing basis; and

- Performing internal assessments of entity-wide risk, both actual and potential, with mitigation strategies.

An annual evaluation, although helpful, should not be the only occasion for risk assessment and monitoring. To ensure that the right controls are in place, it is best to build risk assessment and monitoring into ongoing management processes. Risks facing organizations are continually changing, and a successful system of internal control must be responsive to such changes, enabling adaptation. Effective risk management and internal control are therefore reliant on a regular evaluation of the nature and extent of risks.

In summary, to achieve a strong system of internal control, an organization needs to establish a clear link to risk management. This promotes the most effective and efficient combination of controls necessary to ensure that organizational objectives can be achieved.

**Managing the Internal Control System**

While the governing body or the head of the organization is responsible for ensuring an adequate internal control system is in place, the operation and monitoring of the system of internal control should be undertaken by individuals who collectively possess the necessary skills, technical knowledge, objectivity, and understanding of the organization. Many organizations have established a distinct internal control or risk management function responsible for assessing the risks to the organization and the control system's adequacy in addressing these risks.

The internal control or risk management function is responsible for identifying and inventorying risks to the mission of the organization on both a unit and entity-wide basis. While monitoring these risks and continually reviewing the organization's environment for changes that could impact its mission is an ongoing process, a formal assessment of all inherently high-risk functions should occur at least annually, and lower risk categories should be reviewed at least every three years. The formal report of deficiencies should be directed to the governing body or head of the agency and the audit committee, if one exists. Further, the Internal Control Officer -or in some entities, the Chief Risk Officer - should present enterprise risks based on analysis of reported deficiencies and appropriate review of the internal and external environmental monitoring.

Some organizations also use a senior-level risk management committee, usually consisting of the Internal Control Officer and executives charged with other functions that routinely deal with enterprise risk and risk mitigation (e.g., Counsel, Information Security Officer, etc.). Further enhancement to a risk committee would ideally include key business unit leaders to ensure that the organization's risk efforts are firmly embedded within core business activities. This group may have many responsibilities that range from establishing consistent risk definitions and terminologies, to reviewing reported deficiencies for completeness, and evaluating trend indicators and organizational risk ratings across the organization. In

addition, risk management committees may also:

- Advise on risk strategy: The risk committee serves as a repository of information and expertise on risk and risk strategy. Thus, the risk committee can help inform the organization of risk exposures and advise on future risk mitigation efforts.

- Assist with identifying risk appetite and tolerance: The risk committee can help establish, communicate, and monitor the risk culture, risk appetite, risk tolerances, and risk utilization of the organization at the enterprise and business-unit levels.

- Oversee risk exposures: The risk committee should be continuously aware of the critical risks and exposures facing the organization and of management's strategy for addressing them. The committee should consider the full range of risks and potential interactions among risks, including risk concentrations, escalating and de-escalating risks, contingent risks, and inherent and residual risk.

- Review crisis management plans: The risk committee should keep abreast of the organization's crisis preparedness and ensure that management has developed and can implement a plan to respond to major risks, such as natural disasters, terrorism, cyber-attacks, epidemics, civil disorder, and other events that could compromise the enterprise's human or other resources or disrupt the value chain.

- Support the internal control program: The risk committee can help ensure that the Internal Control Officer has the skills, authority, and resources to oversee risk in the enterprise. The committee can also support the internal control program through consistent communications and actions regarding the organization's approach to risk and risk management.

Whoever is charged with managing and assessing the system of control must understand the nature and context of control, including an understanding of the following:

- The system of internal control should be embedded in the operations of the organization and form part of its culture.

  Control is affected by people throughout the organization, including the governing body, organizational head, management and all other staff. People who are accountable, as individuals or teams, for achieving objectives should also be accountable for the effectiveness of controls that support the achievement of those objectives. It is important that criteria are in place by which the effectiveness of the system of control can be judged. By making individuals accountable, the likelihood that controls will be operated properly is increased.

- Controls should be capable of responding quickly to evolving risks, both internal and external.

  Risks include not only those related to the achievement of a specific objective but also those fundamental to the viability and success of the organization, such as failure to maintain the organization's resilience or capacity to identify and exploit opportunities. Resilience refers to the organization's capacity to respond and adapt to unexpected risks

and opportunities, and to make decisions on the basis of telltale indicators in the absence of definitive information.

- The costs of internal controls must be balanced against the benefits, including the risks they are designed to manage.

  Design decisions involve the acceptance of some degree of risk. The costs of control must always be balanced against the benefits of controlling the risk. It is possible to reach a position where the incremental cost of additional control is greater than the benefit derived from controlling the risk.

- The system of internal control must include procedures for reporting immediately to appropriate levels of management any significant control failings or weaknesses that are identified, together with details of the corrective action being undertaken.

  It should not be assumed, without making appropriate inquiries, that breakdowns in internal controls are isolated occurrences. The key is continual learning rather than attribution of blame. This philosophy should come down from the top of the company. A blame culture encourages the concealment of breakdowns in control. Often, major disasters are the result of the accumulation of a number of smaller, seemingly insignificant events, which if analyzed collectively would have provided the necessary warnings to enable preventive action.

- Controls can help minimize the occurrence of errors and breakdowns but cannot provide absolute assurance that they will not occur.

  Human fallibility and the risk of unforeseeable occurrences are inherent limitations in any system of internal control. A control system cannot be designed to provide protection with certainty against an organization failing to meet its objectives or against all material errors, losses, frauds or breaches of laws or regulations.

**Evaluation**

Evaluation is the process management uses to determine whether:

- the organization will likely achieve its goals and objectives;
- the elements of the organization's internal control system are functioning effectively; and
- risks to the organization and opportunities for improvement are being identified.

It is important to note the distinction between evaluation and monitoring. Monitoring involves performing daily or routine procedures - like supervision, transaction review and problem resolution that help to ensure operations are in compliance with the organization's system of internal control.

Evaluation, on the other hand, involves conducting periodic assessments of the organization's performance compared with established expectations or measurement standards. In New York State government, this usually occurs during the annual certification process for many organizations, but should occur even if an organization is not subject to the Division of the Budget's Budget Policy and Reporting Manual Item B-350, entitled "Government Internal Control and Internal Audit Requirements."

Evaluation can be accomplished through self-assessment and independent review. Regular self-assessment helps management detect problems early, and thus minimizes the costs of these problems. Self-assessments should be scheduled regularly, and should be performed throughout the organization. Self-assessments can include surveys, questionnaires, interviews, observation and specific testing of transactions and key controls. Self-assessments should not only address specific processes, but also evaluate the unit's control environment, communication, monitoring and risk assessment processes.

The frequency of self-assessment should be based, in part, on the results of the organization's risk assessment process. Independent reviews can be performed by external auditors, consultants, and internal auditors who are independent of the operations to be reviewed. Such reviews should not be a substitute for routine self-assessments, but should serve to supplement them.

To perform an orderly, systematic evaluation of an organization's system of internal control, management should segment the organization into "assessable units." Assessable units are not usually the functional subunits found on an organization chart (e.g., bureaus), but are segments of them. For example, a bureau may have five or more assessable units in it, each of which performs a distinct function, program or process.

An assessable unit has certain primary characteristics. It has an ongoing, identifiable purpose that results in the creation of a service or product (used either internally or externally) and/or that fulfills a law, regulation or other mandate. An assessable unit should be large enough to allow managers to evaluate a significant portion of the activity being examined, but not so large that managers cannot perform a meaningful evaluation without extensive time and effort.

Management should maintain an inventory of the assessable units along with the purpose and objectives of each assessable unit, and use it when planning any review of the system of internal control.

The managers of the assessable units should have the responsibility for determining the effectiveness of the system of internal control within their respective units. Managers should ask such questions as:

- Do the unit's objectives provide it with a clear direction?
- Do employees in the unit understand the objectives, and how achievement of the objectives helps to accomplish the organization's mission?
- Does the control environment help to foster achievement of the unit's objectives?
- Does the unit have a means of effectively identifying and managing risk?
- Has unit management established the controls needed to minimize risk?
- Are the controls functioning as designed?
- Are the controls both effective and efficient in accomplishing their purpose?
- Does the unit receive the timely, accurate and useful information needed to achieve its objectives?
- Are communication lines sufficient to meet the needs of senders and receivers of

information?

- Is monitoring within the unit effective in ensuring that daily operations are in compliance with the system of internal control?

- Is the unit effectively monitoring the accomplishment of objectives, the control environment and the communication process?

- Does monitoring adequately identify changes in the internal or external environment?

Management should assess accomplishment of the mission at all levels of the organization on a regular basis. At production or operational levels, management should compare the actual accomplishments of the specific subunits with their operational plans and objectives, as well as, comparing the actual accomplishments of the major organizational divisions with strategic plans and organizational objectives. In addition, any new risks or opportunities that are identified in the assessment process may result in changes to the organization's objectives or modification of its mission.

All aspects of the self-assessment process should be documented, including the evaluation methodologies, the sources and types of information used, reporting relationships, any deficiencies identified, and any corrective action recommended. The results of the assessment should be communicated throughout the organization, and management should have processes in place to ensure that appropriate and prompt actions are taken to address any deficiencies identified. Management should include a review of these corrective actions in a subsequent evaluation process to determine if they have produced the desired outcomes.

## Part IV: Supporting Activities

Strategic planning and internal audit are activities that support a good system of internal control. They provide management with additional tools to help ensure that the mission of the organization will be achieved.

### Strategic Planning

Strategic plans are proposed courses of action designed to enable an organization to achieve its objectives and goals. Planning should begin at the top levels of management with a strategic plan that focuses on the long-range direction of the organization. The strategic planning process should include establishing the organization's broad organizational objectives and developing the strategies that should be followed to achieve them. On the basis of the direction in the organization's strategic plan, management should develop plans for each major organizational division with a long-range focus specific to that division. The division plans guide managers in developing shorter-range operational plans for each of the major functions performed within their respective divisions.

### Objectives

Internal controls need to be tied to specific objectives related to reporting, compliance or operations. Strategic planning helps to define management’s organizational and operational objectives. Management derives organizational objectives from the mission and often develops them during the strategic planning process. They are long-range, broad statements that define the desired outcomes of the organization as a whole. Organizational objectives are necessary for coordinating efforts and evaluating overall performance within an organization. Without these clearly defined objectives, employees could be working inefficiently, ineffectively and/or in conflicting directions.

Good organizational objectives can serve as starting points for more specific and detailed operational objectives within the subunits (i.e., divisions, departments, bureaus and assessable units) of the organization. Operational objectives are shorter range and more specific and define the desired outcomes of each of the organization's subunits. They should be structured in a hierarchy so that each subunit's accomplishment of its operational objectives helps the next higher level achieve its operational objectives, all of which helps management meet its organizational objectives.

All objectives should be in writing. Management should provide employees with written organizational and operational objectives along with the mission statement. Management should ensure that employees understand the objectives and how their work helps to achieve them.

Finally, just as changes in the environment can affect the adequacy and relevancy of the mission statement, these same factors can also affect an organization's objectives. For an organization to function effectively and adapt, it should periodically reassess its organizational and operational objectives.

### Goals

Goals are objectives translated into specific, measurable targets. They are quantifiable and provide a means for assessing the accomplishment of objectives. Management should translate all objectives into attainable goals. Progress toward these goals can help measure accomplishment of an objective. Sometimes it is difficult to translate an objective into a quantifiable goal. In such instances, management should identify some other appropriate indirect measure.

## Operational Plans

Managers at all levels should be able to use operational plans to determine the priority and timing of objectives, to resolve conflicts between objectives, to establish the organization's policies and procedures, and to help set budgets, schedules and resource assignments. Planning should be based on the most objective and accurate information available. All planning processes should identify the most efficient alternatives available for accomplishing the objectives. The plans should be provided to and understood by everyone who must follow them. Management should also establish a process that identifies how and when plans should be changed to reflect both changing conditions and the availability of more accurate information. Plans should be flexible enough to allow for such changes.

## Internal Audit

Internal audit functions add value to an organization's internal control system by bringing a systematic, disciplined approach to the evaluation of risk and by making recommendations to increase the effectiveness of risk management efforts, improve the internal control structure and promote good corporate governance. The Legislature, in passing the Internal Control Act, recognized the internal audit function's key role in supporting the internal control system and, as such, made the Division of the Budget responsible for designating which State agencies would be required to maintain internal audit units. The Division of the Budget makes this determination based in part on the size, nature and/or complexity of agency operations. Other entities may choose to establish an internal audit function as part of their management of risks and resources.

In either case, the Internal Control Act requires that these units be organized and operated in accordance with professional audit standards, in particular *The Standards for the Professional Practice of Internal Auditing* promulgated by the Institute of Internal Auditors. This section, with consideration of the recommendations promulgated in 2006 by the New York State Internal Control Task Force, further interprets those standards as they apply to New York State entities and as such, forms the minimum expectations for the organization and operation of internal audit units within New York State government. Other organizational aspects related to the formation of an internal audit unit, including minimum qualifications for internal audit directors, are addressed by the Division of the Budget in Item B-350 of its *Budget Policy and Reporting Manual*.

## Auditor Independence and Compatibility with Other Duties

A major underlying principle of professional audit standards is that the internal audit function must be organizationally independent of other business activities and free from interference in establishing the scope of its work and the communication of results. This organizational alignment promotes objectivity and allows the auditor to maintain an impartial, unbiased attitude while avoiding conflicts of interest. Internal audit independence and objectivity are important to credibility and are hallmarks of executive management's commitment to promoting a strong, introspective approach to governance. Executive managers, audit committees and third parties need to know that they can rely upon the internal auditor's independence when considering his or her findings and recommendations.
To ensure independence and objectivity, the internal audit function should report to the highest level of governing body charged with the responsibility to direct and/or oversee the activities and management of the organization. Ideally then, the function should be organized under the chief executive and report directly to any audit committee, board of directors or other governing authority that may exist.

Auditor independence also entails refraining from duties that are incompatible with the objective appraisal

of operations. Internal auditors should therefore avoid assuming operational responsibilities or engaging in other activities that may impair their independence, including functioning as their entity's Internal Control Officer (ICO). On the most basic level, the ICO duties are defined as working with appropriate agency personnel to coordinate the internal control activities, and to ensure that the agency's internal control program meets the requirements established in agency policy. The ICO role is therefore a management function that requires decisions about the overall design and implementation of the internal control system; as such, it is generally incompatible with the role of the internal auditor. Similarly, internal auditors should also avoid functioning as their entity's Information Security Officer (ISO), as this role not only requires specialized expertise, but can also require the auditor to perform management functions or make management-level decisions.

Although it is critical for agencies and other government organizations to preserve the independence of their internal audit operations, as a practical matter, some may experience temporary situations whereby they have insufficient resources to fully separate internal audit from their internal control and information security functions. In these situations, the internal auditor should limit his/her role to the extent possible, being careful to avoid decision making in areas such as the specific type of controls needed or the quality of controls in place. For example, if the internal auditor undertakes any internal control responsibilities, executive management needs to clearly reinforce that agency managers are the individuals responsible for maintaining an appropriate system of internal controls. Further, the agency's annual internal control certification, as well as any subsequent audits of the internal control system, should each fully disclose the internal auditor's role in the internal control process.

Separation of the internal control and internal audit functions does not preclude a strong working relationship that can create synergies between the two activities. Creating a sense of cooperation between the internal control and internal audit functions will improve the overall internal control culture of an agency. The internal control and internal audit functions reinforce one another when:

- The internal auditor uses internal control reports when planning audits;
- The auditor consistently evaluates and reports on compliance with internal control requirements in audit reports, as part of the auditor's assessment of internal controls;
- The ICO reviews internal audit reports on a regular basis to ensure that agency managers incorporate significant risks, findings and recommendations into the internal control system; and
- Follow-up audits address whether significant risks, findings and recommendations have been addressed and incorporated into the agency's internal control system.

Adopting these steps will provide the internal auditor and ICO with continuous feedback on the quality of the internal control system and, as a result, lower the risk that the system may be ineffective or lose its effectiveness over time.

Maintenance of auditor objectivity also requires a continuing assessment of each auditor's relationship with the operations she or he audits. Internal audit units therefore need to establish procedures to identify personal impairments, and should obtain information concerning potential conflicts of interest and bias from audit staff at least annually. Auditors should also immediately report any new impairment that arises to their internal audit director.

**Risk-Based Audit Planning**

Internal audit units exist in New York State due in major part to the provisions of the Internal Control Act, which focuses largely on control systems internal to the entity. In fact, the Act specifically requires that the internal audit function shall evaluate the agency's internal controls and operations. To fulfill this responsibility, internal audit units must devote resources to examining their organizations' internal operations and cannot simply audit outside parties that conduct business with their organizations, such as contractors, grantees or service providers. Still, the Act does not specify the minimum level of audit resources that must be devoted to internal activities, and there is no expectation that all internal audit resources be directed internally. Rather, the appropriate allocation is best determined as part of a larger analysis of risks facing the particular entity.

The Director of Internal Audit in each State agency also must periodically develop a risk-based plan of audit engagements to determine the priorities for the internal audit activity. This audit plan must be based on a risk assessment, which is updated at least annually. As part of this assessment, the internal audit unit should review and test documentation maintained by the agency's Internal Control Officer in support of the entity's annual certification. Depending on the results of these tests, the internal audit unit may be able to form a basis to rely on the certification or may decide to set it aside and conduct its own separate review of internal controls. When audits of internal control systems are performed, the auditor should identify the specific objectives of the examination and should consider examining each of the five elements of internal control along with their related principles as discussed in these Standards: control environment, risk assessment, control activities, information and communication, and monitoring. Depending on the needs of the agency, the audit unit may need to expand the scope of its inquiry even further.

Input from senior management and the governing board (where applicable) must also be considered in the audit planning process to ensure the plan of engagements is consistent with the organization's goals. Further, the auditor should share information and coordinate activities with other internal and external providers of relevant assurance and consulting services, both to ensure proper coverage and to minimize duplication of efforts. The Director of Internal Audit should communicate the audit plan and the associated resource requirements, including any significant interim changes, to senior management and to the board for review and approval. The Director of Internal Audit should also communicate the impact of any resource limitations and should ensure that internal audit resources are appropriate, sufficient, and effectively deployed to achieve the approved plan.

**Continuing Professional Education**

To be effective in a changing world, all audit staff need to maintain and enhance their technical competence through a program of continuing education. Professional audit standards, as well as various professional licensing programs including the Certified Internal Auditor and the Certified Public Accountant, all include periodic continuing education requirements. The Internal Control Task Force report provides an extensive discussion on the need for continuing education and training of the State's internal auditors. The consensus recommendation is that each auditor is required to obtain at least 80 hours of continuing professional education every two years, with not less than 20 hours obtained during any single year. This requirement is consistent with the level of training required of other professionals conducting audits of government programs. The Task Force report appendix entitled Guidance on Continuing Education Requirements for New York State Internal Auditors provides a more detailed discussion of these requirements, and is incorporated by reference as part of these Standards.

**Communication**

Communication is also a critical factor in ensuring that internal audit operations provide maximum value to the organization. Professional standards require periodic meetings between the internal auditor, executive management and any governing board or audit committee that may exist. These meetings are essential to ensure the independence, effectiveness and accountability of the internal audit activity and should be held at least quarterly. The timely distribution of internal audit reports is another integral way that communication supports the independence, effectiveness and credibility of the internal audit organization. Distributing the audit reports to all stakeholders, including executive management, provides reasonable assurance that the agency will take action on the findings and recommendations contained therein. The internal audit director should be responsible for the distribution of each audit report and should provide copies to the agency head, the deputy head, the internal control officer, the audit committee (if applicable) and the head of the audited operation. Any further distribution of audit reports should be made only with the knowledge and permission of executive management.

**Monitoring Audit Findings**

The Internal Control Act requires internal auditors to identify internal control weaknesses that have not been corrected and make recommendations to correct those weaknesses. To accomplish this, each unit needs to establish and maintain a system to monitor the disposition of audit recommendations communicated to management. The auditor should document the rationale in deciding which audit recommendations should be followed up on and when, in contrast with recommendations where no follow-up is needed. The auditor should also follow up with management to document either that audit recommendations have been effectively implemented, or that senior management has accepted the risk of not implementing the recommendations. To the extent agreed upon with management, the internal audit unit should also monitor the disposition of recommendations arising for any non-audit services.

**Maintaining Audit Documentation**

Internal audit units should maintain documentation for each audit and subsequent follow-up. This documentation should contain sufficient information to enable an experienced auditor who has no previous connection with the audit to ascertain the evidence that supports the auditors' significant judgments and conclusions. Each internal audit unit should establish a formal policy that clearly delineates who is responsible for reviewing audit documentation prepared by various staff levels and when that review should occur.

Audit documentation is the auditors' property and should be kept under their control. The auditors should know exactly where all pieces of documentation are at all times during the conduct of the audit. Approval from senior management and/or legal counsel should be obtained prior to releasing copies of audit documentation and reports to external parties. When not in use, documentation should be kept in a locked file or otherwise secured so as not to be readily available to persons who are not unauthorized to access it. This includes protecting electronic information with appropriate IT security controls. Audit documentation should be retained for a minimum of seven years after the date of the audit report. For recurring audits, the documentation supporting previous audits may be filed in a centralized record retention facility provided an individual is assigned to maintain a record of the location of each item sent to record storage and an appropriate destruction date is scheduled for the material.

**External Quality Assessment Review**

Professional audit standards require each internal audit organization to periodically undergo an independent review of the quality of its audit activities. The purpose of this review is to ensure that the organization's quality control system is suitably designed and consistently complied with to the extent necessary to reasonably ensure compliance with audit standards. External assessments also promote more effective and efficient internal auditing operations by identifying better practices and making recommendations intended to improve performance. Periodic quality assessments are also an important means of reinforcing management's confidence in the work of the internal audit unit. As such, each internal audit unit in New York State government must have an appropriate external quality assessment review performed at least once during every five-year period.

## APPENDIX B

## New York State Energy Research and Development Authority

CODE OF CONDUCT

## A Guide for NYSERDA Employees

### Introduction

To maintain the confidence of the public, all NYSERDA employees shall conduct business in an honest and ethical manner, reflecting such values as integrity, fairness, and trustworthiness. This Code of Conduct summarizes a number of basic standards and State and Federal laws that NYSERDA employees and Board Members of NYSERDA are required to follow while acting in that capacity on behalf of the organization.

This Code of Conduct is not intended to cover all situations and answer all questions. Additional administrative guidance and direction can be found in NYSERDA's policy and procedure manuals. Legal guidance and direction is available through NYSERDA's Ethics Officer, who is an attorney in the Counsel's Office. Questions about a specific situation should be directed to your supervisor, the Director of Internal Audit, the Manager of Human Resources, the Counsel's Office, or NYSERDA Officers. Additionally, you may contact the New York State Joint Commission on Public Ethics directly about any questions or issues.

### General Conduct

You are expected to maintain the standards of conduct described in this Code of Conduct. You must:

- Conduct yourself in a manner that is consistent with NYSERDA policies and procedures and the State and Federal laws that apply to you as a NYSERDA employee.
- Conduct yourself in a manner that is consistent with the public trust and the proper performance of your duties, including refraining from engaging in outside activities that would impair your independence of judgment.
- Conduct business with NYSERDA contractors in a manner that does not give the impression that any person can improperly influence you or unduly enjoy your favor.

*(See Personnel Handbook Section 2 and cited references)*

### Conflicts of Interest

As a public employee, you are bound by the Public Officers Law and must endeavor to pursue a course of conduct that will not raise suspicion among the public that you are likely to be engaged in acts of violation of your public trust. You must not use your official position to secure special privileges for yourself or others or engage in outside business activities that might interfere with or compromise your ability to perform your official NYSERDA duties. Actual or potential conflicts of interest with individuals or entities doing business with NYSERDA should be disclosed to supervisory personnel immediately *(See Appendix C: Whistleblower Policy).*

You may not engage in outside activities that would conflict with scheduled work hours or that would impair your judgment or compromise or interfere with your ability to properly perform your duties. You may not use NYSERDA time, materials, equipment, or other assets in connection with outside activities. NYSERDA employees who are designated policymakers must obtain approval before engaging in any outside activity if the amount to be earned exceeds $1,000 annually.

The New York State Joint Commission on Public Ethics publishes opinions concerning the Public Officers Law, including what constitutes a conflict of interest and can be an additional source of guidance. *(See Personnel Handbook Section 2 and the references cited in Section 2)*

## Improper Gifts

No gift of **any** value may be accepted if it would constitute a substantial conflict with the proper discharge of your duties. In addition, Section 73(5) of the Public Officers Law prohibits you from directly or indirectly soliciting, accepting, or receiving any gift that has more than nominal value where the circumstances would reasonably permit the inference that the gift:

- was intended to influence you, or could reasonably be expected to influence you, in the performance of your duties; or
- was intended as a tip, reward, or sign of appreciation for your official action.

A gift may be in many forms including, but not limited to, money, property, service, loan, travel, meals, special favors, refreshments, entertainment, hospitality, promise, or discount.

The New York State Joint Commission on Public Ethics has issued regulations on gifts, and issues opinions concerning the Public Officers Law, including what constitutes acceptable and unacceptable gifts, and can be an additional source of guidance. *(See Personnel Handbook Section 2, the cited references in Section 2 and Appendix B, and the New York State Joint Commission on Public Ethics opinions and interpretations)*

## Discriminatory Practices or Harassment

Discriminating against or harassing other employees or contractors on the basis of race, religion, sex, national origin, age, disability, marital status, or sexual orientation is strictly prohibited. *(See Personnel Handbook Section 11 and the references cited in Section 11)*

### Confidential Information

Confidential, proprietary, and trade-secret information acquired by you in the course of your official duties may not be disclosed or used to further your or another's personal interests, including financial interests. *(See Public Officers Law section 74(3)(c), Personnel Handbook Section 2 and cited references, and Operations and Procedures Handbook Section 4.5)*

### Financial Interests

You should not retain or obtain a financial interest in any person or organization that does business with NYSERDA if you are or are likely to participate or be involved in the decision-making process at

NYSERDA in a matter involving that person or organization.

You should not provide inside information to any person except in carrying out NYSERDA's corporate purposes, or give advice or make recommendations or suggestions to another person on the basis of inside information. *(See Personnel Handbook Appendix B)*

## Controlled Substances and Alcohol

The sale, attempt to sell, possession, or purchase of non-prescribed controlled substances while at the workplace or while performing in a work-related capacity is prohibited. Employees also are prohibited from being impaired by controlled substances or alcohol while on the job or on the work site. *(See Personnel Handbook Section 17)*

## Use of NYSERDA Assets

You are expected to use all equipment, materials, and other office property in a responsible manner. Employees should not use NYSERDA time, property, equipment, or supplies for personal use or private gain. This includes, but is not limited to, NYSERDA's telephones, computer systems, personal digital assistants, stationary, supplies, copiers, postage, internal office, mail, inter-city couriers, and vehicles. Certain personal use is not prohibited when it is incidental, necessary, and limited in number and duration, such as the reasonable personal use of telephones and electronic mail, and does not conflict with the proper exercise of the employee's duties. NYSERDA's President and CEO has unrestricted use of NYSERDA fleet vehicles, as provided in and subject to the requirements of the NYS Division of Budget's Policy D-750 on State Vehicles. (*See Personnel Handbook Section 2)*

## Political Activity

Employees are under no obligation to contribute to any political fund or perform any political service. Employees may not use job-related influence to force political activity on the part of others nor may others make the demand on them. You may not require employees or potential employees and contractors or potential contractors to reveal information on party affiliation or campaign contributions. Should you intend to run for political office, you should obtain your supervisor's and Counsel's Office concurrence that the public office to be sought will not interfere with your official NYSERDA duties and is allowed under State and Federal Law. Policymakers seeking public office for which more than nominal compensation will be paid must first obtain the approval of the New York State Joint Commission on Public Ethics. *(See Personnel Handbook Section 2 and State Ethics Commission regulations Section 932)*

## Reporting Violations

In accordance with NYSERDA's Whistleblower Policy, you must remain alert to possible violations of law, policy, or public trust, everywhere in NYSERDA. Section 55(1) of the Executive Law requires all state officers and employees to promptly report to the State Inspector General any information concerning corruption, fraud, criminal activity, conflicts of interest, or abuse by another state officer or employee relating to his or her employment.

You must cooperate in any official investigation of a violation.

Retaliation against any employee who in good faith reports a violation of law, policy, or public trust is prohibited. *(See Whistleblower Policy and Personnel Handbook Section 11)*

**Resources Available**

Internal
Mark Mitchell, Director of Internal Audit
Jeff Pitkin, Internal Control Officer
Noah Shaw, General Counsel (and all other Counsel's Office staff)

External
Fraud and Abuse Hotline 1-866-219-1122
NYS Joint Commission on Public Ethics 518-408-3976
NYS Office of the Inspector General 1-800-367-4448
Authorities Budget Office 1-800-560-1770

## APPENDIX C

## WHISTLE BLOWER POLICY
**April 2012**

PURPOSE

It is the policy of NYSERDA to afford certain protections to individuals who, in good faith, report violations of NYSERDA's Code of Ethics or other instances of potential wrongdoing within NYSERDA. The Whistleblower Policy and Procedures set forth below are intended to encourage and enable employees to raise concerns in good faith within NYSERDA and without fear of retaliation or adverse employment action.

DEFINITIONS

Good Faith: Information concerning potential wrongdoing is disclosed in "good faith" when the individual making the disclosure reasonably believes such information to be true and reasonably believes that the information constitutes potential wrongdoing.

NYSERDA Employee: All NYSERDA board members, officers, and staff whether full-time, part-time, employed pursuant to contract, employees on probation, and temporary employees.

Personnel action: Any action affecting compensation, appointment, promotion, transfer, assignment, reassignment, reinstatement, or evaluation of performance.

Whistleblower: Any NYSERDA Employee who in good faith discloses information concerning wrongdoing by another NYSERDA Employee, or wrongdoing concerning the business of NYSERDA itself.

Wrongdoing: Any alleged corruption, fraud, criminal or unethical activity, misconduct, waste, conflict of interest, intentional reporting of false or misleading information, or abuse of authority engaged in by a NYSERDA Employee that relates to NYSERDA.

SECTION I: REPORTING WRONGDOING

All NYSERDA Employees who discover or have knowledge of potential Wrongdoing concerning board members, officers, or employees of NYSERDA; or a person having business dealings with NYSERDA; or concerning NYSERDA itself, shall report such activity in accordance with the following procedures:

a) All NYSERDA Employees who discover or have knowledge of Wrongdoing shall report such Wrongdoing in a prompt and timely manner.

b) The NYSERDA Employee shall disclose any information concerning Wrongdoing either orally or in a written report to his or her supervisor, or to the Director of Internal Audit, an Officer, any member of Counsel's Office, an independent Fraud and Abuse Hotline service available to NYSERDA employees, the Ethics Officer, a representative from human resources.

c) The identity of the whistleblower and the substance of his or her allegations will be kept confidential to the maximum extent possible.

d) Upon receipt of an allegation of Wrongdoing, the individual to whom the potential Wrongdoing is reported shall notify the General Counsel, and the General Counsel shall determine who will conduct the investigation. Once the investigation is complete, the General Counsel or the individual who conducted the investigation shall provide to the President and CEO a summary report, which shall include a recommendation for resolving the matter. The Director of Internal Audit shall advise the Audit and Finance Committee at its next regularly scheduled meeting of any material or significant weaknesses or deviations identified in such report.

e) The individual to whom the potential Wrongdoing is reported may refer such information to the Authorities Budget Office or an appropriate law enforcement agency where applicable.

f) Allegations of corruption, fraud, criminal activity, conflicts of interest or abuse by a NYSERDA Employee or any persons having business dealings with NYSERDA must be reported to the State Inspector General.

g) All NYSERDA Employees shall cooperate fully with internal investigations and investigations by the State Inspector General pertaining to NYSERDA operations.

h) All reports and draft reports delivered to NYSERDA by the State Inspector General shall be reviewed by the Audit and Finance Committee, which shall serve as the point of contact on such reports.

i) Should a NYSERDA Employee believe in good faith that disclosing information within NYSERDA pursuant to Section 1(a) above would likely subject him or her to adverse personnel action or be wholly ineffective, the NYSERDA Employee may instead disclose the information to the Authorities Budget Office or an appropriate law enforcement agency, if applicable. The Authorities Budget Office's toll free number (1-800-560-1770) should be used in such circumstances.

SECTION II: NO RETALIATION OR INTERFERENCE

No NYSERDA Employee shall retaliate against any Whistleblower for the disclosure of potential Wrongdoing, whether through threat, coercion, or abuse of authority; and, no NYSERDA Employee shall interfere with the right of any other NYSERDA Employee by any improper means aimed at deterring disclosure of potential Wrongdoing. Any attempts at retaliation or interference are strictly prohibited. In addition:

a) No NYSERDA Employee who in good faith discloses potential violations of the NYSERDA Code of Conduct or other instances of potential Wrongdoing, shall suffer harassment, retaliation or adverse personnel action as a result of such disclosure.

b) All allegations of retaliation against a Whistleblower or interference with an individual seeking to disclose potential Wrongdoing shall be thoroughly investigated by NYSERDA.

c) Any NYSERDA Employee who retaliates against or attempts to interfere with any individual for disclosing or attempting to disclose potential violations of the NYSERDA Code of Conduct or other instances of potential Wrongdoing is subject to discipline, which may include termination of employment.

d) Any allegation of retaliation or interference will be taken and treated seriously and irrespective of the outcome of the initial complaint, such allegation will be treated as a separate matter.

SECTION III: OTHER LEGAL RIGHTS NOT IMPAIRED

The Whistleblower Policy and Procedures set forth herein are not intended to limit, diminish, or impair any other rights or remedies that an individual may have under the law with respect to disclosing potential Wrongdoing free from retaliation or adverse personnel action.

a) Specifically, these Whistleblower Policy and Procedures are not intended to limit any rights or remedies that an individual may have under the laws of the State of New York, including but not limited to the following provisions: Civil Service Law § 75-b, Labor Law § 740, State Finance Law § 191 (commonly known as the "False Claims Act"), and Executive Law § 55(1).

b) With respect to any rights or remedies that an individual may have pursuant to Civil Service Law § 75- b or Labor Law § 740, any NYSERDA Employee who wishes to preserve such rights shall prior to disclosing information to a government body, have made a good faith effort to provide the appointing authority or his or her designee the information to be disclosed and shall provide the appointing authority or designee a reasonable time to take appropriate action unless there is imminent and serious danger to public health or safety. (See Civil Service Law § 75-b[2][b]; Labor Law § 740[3]