

## **INTERNAL CONTROL DEFINITIONS**

**Assessable Unit** – Assessable units are not usually the functional sub-units found on an organization chart, but are segments of them. 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. Examples of an assessable unit are academic and administrative departments or units within the vice presidents' divisions.

**Assessing Risks** – Risks are events that threaten the accomplishment of objectives. There are both internal and external risks. Examples of risks include human error, fraud, system breakdowns and natural disasters. The risk assessment process involves identifying each risk in terms of:

- **Likelihood** – The probability that an unfavorable event would occur if there were no internal controls or limited internal controls.
- **Significance or Impact** – A measure of the magnitude of the effect on an organization if the unfavorable event were to occur. Inherent risk is innate to the program function or activity and is evaluated by the ultimate harm that may be done or the opportunity that may be lost.
- **Cause** – The reason why an unfavorable event may occur.

**Cash** – College funds are defined as cash and cash equivalents (“cash”) and include currency and coins, personal checks, business checks, traveler’s checks, cashier’s checks, money orders, credit/debit card transactions, electronic payments including Automated Clearing House (ACH), and wire transfers.

**Cash Management** – The use of proper procedures and Internal Controls when handling cash collections and deposits. Procedures are designed to provide reasonable assurance that errors will be detected and corrected in the normal course of activities, and to prevent mishandling of funds, safeguard against loss, and protect employees from inappropriate charges by defining responsibilities in the cash handling process.

**Certification** – According to the Internal Control Act and Division of the Budget’s (DOB) Budget Policy and Reporting Manual (BPRM) Item B-350, State agencies and covered authorities are required to perform certain Internal Control responsibilities (as outlined in the definition for Internal Control Act). Each year, DOB issues a Budget Bulletin to SUNY, which is forwarded to the Colleges, that contains the “Internal Control Certification” form along with a request for additional information in support of the College’s certification which is to be provided and submitted along with the certification document. The President signs and submits the compliance certificate to SUNY on or before March 31 annually. Through this certification document, the College’s official is affirming that SUNY Brockport has complied with the specific responsibilities listed in the Internal Control Act.

**Communication** – The exchange of information between and among people and organizations.

- A communication system consists of methods and records established to identify, capture and exchange useful information. Characteristics of a good communication system: timely information is provided when the user needs it; sufficiently detailed information to help the user achieve his or her objectives; and information should be tailored to the user.

- Management should have clear internal communication channels that: inform employees of their duties and responsibilities; report 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 must be taken seriously.
- In the organization, good communication channels should allow management the means to tell employees: about the organization's goals, objective, policies and plans; about their job descriptions, including the purpose of their work, how the employee's efforts are linked to the organization's strategic plan, and how employees contribute to achieving the organization's mission.
- Communication in the control environment – Management should establish mechanisms for employees to report sensitive matters without retribution. Sensitive matters include improper acts and unethical behavior. To preserve effective communication, management should be receptive to negative messages such as employee complaints and unfavorable customer feedback.
- Other elements of communication include: assessing and managing risks, control activities, monitoring and evaluating.

**Control Activities** – Policies and procedures that help ensure objectives are achieved and the tools, both manual and automated, that help prevent or reduce the risks that can impede accomplishment of the organization's mission. Control activity consideration:

- The cost of the control activity should not exceed the cost incurred if the undesirable event occurred
- Build control activities into business processes and system as the processes and systems are being designed
- The distribution of resources among the control activities should be based on the significance and likelihood of the risk it is preventing or reducing.

Commonly used control activities include: documentation, approval and authorization, verification, supervision, separation of duties, safeguarding assets, and reporting.

Control activities for computer systems for the non-systems manager include:

- Backup and disaster recovery
- Input controls such as edit checks, key verification, redundancy checks, echo checks, and completeness checks.
- Output controls which include changes made to the master file, error listing, distribution registers, end-of-job markers, and a quality assurance review.

**Control Environment** – Also referred to as “general control environment,” is the atmosphere created by the people of an organization, which sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity, ethical values, and competence of the organization's people; management's philosophy and operating style; the way management assigns authority and responsibility, and organizes and develops its people. It has a pervasive influence on all the decisions and activities of an organization, and on the control consciousness of its people. The control environment is the foundation for all the other components. The components of the Control Environment are:

- Ethical Values and Integrity
  - Examples include commitment to honesty and fairness, recognition of an adherence to laws and policies, respect for the organization, commitment to excellence, respect for authority, respect for employees' rights, and conformance to professional standards.
  - Management encourages integrity by: setting the example, 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.
- Management Operating Style and Philosophy – Actions reflect management's basic beliefs regarding how the people and activities of an organization should be managed. There are many styles and philosophies – none are inherently right or wrong; some may be more effective than others. Elements affecting the entity's philosophy and style include the degree to which management is willing to accept risks, the degree of economic or regulatory control imposed by others, and the attitudes toward reporting (both financial and programmatic) and accountability.
- Competence – The characteristic of people who have the skill, knowledge, ability and tools to perform a task. Management must ensure that staff possess the knowledge, skills and ability necessary to do their jobs. Management must ensure that staff have what they need – such as equipment, software and policy and procedure manuals. Management should 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, and establishing training programs that help employees increase their knowledge and skills.
- Morale – The attitude people have about their work, as exhibited by their confidence, their discipline, enthusiasm and their willingness to perform tasks. Management is responsible to maintain good morale. Staff should have the 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 objective of the organization; and the lines of communication are open.
- Supportive Attitude – Executive management should be a tone that emphasizes the importance of internal controls, including: ongoing education to ensure everyone understands the internal control system and their role in it; an openness to control self evaluations and internal and external audits of controls; responsiveness to issues raised as the result of the evaluations and audits; and minimal and guarded use of control overrides.

**Cost of Internal Control** – Internal control systems should remain cost effective and not exceed the benefit derived.

**Evaluation** – The process management uses to assess whether an organization's operations are effective in achieving its mission. Evaluation provides reasonable assurance that the organization will likely achieve its mission, plans, objectives and goals; the elements of the organization's system of internal control are functioning effectively; and they can identify both risks to the organization and opportunities for improvement. The basis for evaluation is self-assessment and independent assessment.

**Event Cycle (Process)** – A series of related activities that are performed which account for an event from start to finish, such as the procurement cycle, which encompasses everything from department requisitioning, purchasing, receiving, accounts payable, and inventorying.

**Fraud Reporting** – The reporting of observed or suspected fraud, waste, abuse or irregular activities. These activities include improper transactions, such as suspected thefts, losses, embezzlements, misappropriations, or inappropriate action involving State funds, equipment, supplies or other assets. Also included would be falsification of College records in furtherance of a fraudulent scheme.

**Inherent Risk** – The potential for waste, loss, abuse, and/or mismanagement due to the nature of the function/activity, or the nature and type of resources associated with the function/activity, without regard to controls.

**Internal Accounting Controls** – Procedures used to make sure that assets of the organization are protected and that its financial and accounting records are accurate and reliable. Accounting controls should be in place over all identified business areas and functions.

**Internal Administrative Controls** – These procedures encourage adherence to policies and promote efficiency in the daily operation and management of an organization. Examples of these types of controls are administrative manuals, organization charts, formal job descriptions and hiring practices.

**Internal Audit** – An independent appraisal activity supported by management to review an organization's operations as a means of assuring conformance with management policies and the effectiveness of internal control systems. An internal audit tests the reliability of the internal control system, identifies material weaknesses, and includes recommendations to improve those controls to promote adherence to prescribed policies and procedures.

**Internal Control Act** – Referred to as the New York State Governmental Accountability, Audit and Internal Control Act (originated in Chapter 814 of the Laws of 1987, then made permanent in Chapter 510 of the Laws of 1999), is the basis for the SUNY Brockport Internal Control Program. The Internal Control Act requires that all State agencies, including SUNY, institute a formal internal control program.

There are six requirements of the Internal Control Act, only five of which apply to SUNY Brockport:

- Establish and maintain guidelines for a system of Internal Controls.
- Establish and maintain an Internal Control system and Internal Control Review Process.
- Make a clear and concise statement of managerial policies and standards available to all employees.
- Designate an Internal Control Officer.
- Provide Internal Control education and training.

**Internal Control Advisory Committee** – A committee that is composed of individuals from a cross section of campus departments and offices to provide a central and consistent authoritative body for the review and approval of the College's internal controls.

**Internal Control Coordinator** – An individual who assists the Internal Control Officer with the administration of the Internal Control Program.

**Internal Control Officer** – An individual with sufficient authority to act on behalf of the campus President to ensure implementation and review of the campus Internal Control Program.

**Internal Control Program** - The College at Brockport's Internal Control Program is essentially a program of review. The Program helps to ensure that daily operating practices and procedures are sufficient to minimize the possibility of operational failure, overspending or other actions inconsistent with policy or in violation of the law. Simply stated, the College's Internal Control Program is designed to review, critique and strengthen our existing systems and procedures.

**Internal Control Review** – An internal control review analyzes procedures and policies to ensure they are functioning as intended and that they assist the unit in meeting its objectives and goals. Examples of procedures and policies which may be reviewed include planning activities, program evaluations, the budget cycle, personnel transactions, information systems, cash activities, contract management and capital programs.

**Internal Control Summary** – A brief overview of the major Internal Control activities undertaken during the year, including a description of the management actions to strengthen Internal Controls, and a synopsis of key findings and corrective actions.

**Internal Control Systems** – The Internal Control Program is comprised of several major internal control systems. These systems support and strengthen the College's planning processes and provide reasonable assurance that the objectives of our Internal Control Program are met. Some examples of the major internal control systems now in place include: administrative procedure manuals, budget development and approval process, cash controls, chart of accounts, computer operations/ Information Technology, Environmental Health and Safety, equipment inventory system/Property Control, Financial Aid, formal statements and polices governing hiring procedures, Human Resource policy handbooks and memoranda, institutional data coordination, Internal Control review activity, mission statements and operational objectives, New York State Education Law and other applicable laws, policies and regulations, organization charts and decision-making hierarchies, pandemic planning/disaster recovery, and procurement.

**Internal Control Testing** – An examination of a sample of transactions or events to determine if the desired outcomes have occurred. The sample selection should be without bias to determine objectively that the internal controls in place are adequate, effective, and functioning as intended.

**Internal Controls** – The steps taken by an organization to provide reasonable assurance that the organization functions in an efficient and appropriate manner consistent with its policy objectives, applicable laws, regulations, and related policies and procedures. The methods used to successfully organize and manage daily operations. Internal controls are an integral part of the operating procedures management uses to achieve its objectives and prevent undesirable results.

Internal control is the integration of the activities, plans, attitudes, policies, and efforts of the people of an organization working together to provide reasonable assurance that the organization will achieve its objectives and mission.

This definition establishes that internal control:

- impacts every aspect of an organization: all of its people, processes, and physical structures;

- is a basic element that permeates an organization;
- incorporates the qualities of good management;
- is dependent upon people and will succeed or fail depending on the attention people give to it.

**Monitoring** – The process that assesses the quality of internal control performance over time. Monitoring is the ongoing review of the organization’s daily activities and transactions to determine whether controls are effective in ensuring that operations work as intended. Monitoring responsibilities and duties for:

- Staff – Monitors own work to ensure it is being done properly; correct the errors they identify; detect problems with existing control activities; and report changes in their immediate internal and external environments.
- Supervisors – Monitoring focus should be on ensuring that 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.
- Middle Management – Monitoring responsibilities should cover the review of how well controls are functioning in multiple units within an organization, and how well the supervisors are performing monitoring in the respective units. These managers’ focus should be similar to that of supervisors, but extended to cover all the units for which they are responsible.
- Executive Management – Focus is on major divisions of the organization with more emphasis on monitoring the organization’s achievement of its goals. Executive management monitor for the existence of risks and opportunities in either the internal or external environment.

**Organization** – Helps people focus in a way that brings their various functions together into an orderly, functional and structured whole. Organization components include:

- Strategic plans – the courses of action that will enable an organization to achieve its mission, objectives and goals
- Mission – the organizations’ reason for existing
- Objectives – the organizations desired outcomes
- Goals – are objectives translated into specific, measurable targets
- Operational plans – used to determine the priority and timing of objectives, to resolve conflicts between objectives, to establish the organizations’ policies and procedures, and to help set budgets, schedules and resource assignments
- Structure – the framework in which the organization’s plans are carried out
- Assessable units – segments of the organization which perform a distinct function

**Preventative Controls** – Controls designed to keep errors or irregularities from occurring in the first place. They are built into internal control systems and require a major effort in the initial design and implementation stages. Once in place, these controls do not require significant ongoing investment.

**Reasonable Assurance** – All internal control systems must provide reasonable assurance that the objectives of the departments and units will be met in a cost effective manner. Reasonable assurance provides sufficient confidence that internal controls are functioning to ensure that these parts of the organization will meet their goals and objectives.

**Risk (Vulnerability)** – Significant condition resulting from no action being taken, the wrong action being taken, or the right action not taken in a timely manner, that could impede an organization/department from achieving its goals and objectives. The likelihood that errors and irregularities will occur and/or go undetected considering the quality of existing internal controls or the absence of internal controls, as compared to the inherent risk associated with the function/activity.

**Risk Assessment (Vulnerability Assessment)** – The identification and analysis of relevant risks that may prevent an entity from achieving objectives. It is the basis for determining how that risk should be managed, and the methodology followed to determine the relative susceptibility of programs, functions, or organizational entities to conscious or unintended abuse, misuse through misappropriation of assets, accounting or reporting errors, or reduced operational efficiency. Risk analysis is another term for this type of activity.

**Risk Management** – A program or process designed to accept, avoid, control, share or transfer risks in order to achieve an organization’s objectives.

**Segmentation** – The process of identifying the program and administrative functions necessary for the College to carry out its mission. Functions identified through this process are called “assessable units” and provide the framework for the implementation of the College’s Internal Control Program.

**Separation of Duties** – Key duties and responsibilities in authorizing, processing, recording and reviewing transactions are separated among individuals.

09/17/07