

GLOSSARY - Consolidated

Accounting Controls - Methods and procedures which an organization's management institutes to (1) safeguard assets, (2) authorize transactions, (3) monitor financial activities, and (4) ensure the accuracy and validity of accounting records.

Administrative Controls - Methods through which management supports the accomplishment of its objectives (e.g., planning, organizing, monitoring productivity, improving operations, and ensuring quality control). These controls are necessary to ensure that:

- All resources, including personnel, are properly obtained, maintained, and used;
- Decisions regarding the expenditure of funds are made based on reliable information; and,
- Budgets are properly developed and monitored to ensure consistency between planned and actual expenditures.

Application Controls - Programmed procedures in application software and related manual procedures, designed to help ensure completeness and accuracy of information processing. Examples include computerized edit checks of input data, numerical sequence checks, and manual procedures to follow up on items listed in exception reports. These controls vary based upon the business purpose and specific application to which they apply. Application controls may also help ensure the privacy and security of data transmitted between applications.

Assessable Unit - An organizational, functional, programmatic, or other applicable subdivision of an organization that allows for adequate internal control analysis.

Audit Committee - A group formed by the governing body to oversee audit operations and circumstances. The Committee selects and appraises the performance of the external auditors. The Committee may be composed of outside directors. Besides evaluating external audit reports, the Committee may evaluate internal audit reports as well. Management representations are also reviewed. The Committee may also get involved with public disclosure of the government's activities. The Audit Committee may also, under some circumstances, intervene in the resolution of deficiencies uncovered during an audit.

Cash - A current asset account which includes currency, coins, checking accounts, and undeposited checks received from customers.

Change Fund - An amount of cash held by a department or office and used to give change to customers when they are paying for goods or services.

COBIT – Control Objectives for Information and Related Technology. An IT-focused control framework issued by ISACA.

Compliance - Conforming with laws, rules, and regulations applicable to an entity.

Computer Controls - Controls performed by computer; i.e., controls programmed into computer software (contrast with Manual Controls). Controls over computer processing of information, consisting of general controls and application controls (both programmed and manual).

GLOSSARY - Consolidated

Control – A policy or procedure, inherent in an entity’s organizational structure, hierarchy of authority, or system of work flows, designed to help an entity accomplish its objectives. The effects of such policies and procedures. The act of implementing such policies and procedures.

Control Account – A control account is a summary account in the general ledger. The details that support the balance in the summary account are contained in a subsidiary ledger—a ledger outside of the general ledger. The purpose of the control account is to keep the general ledger free of details, yet have the correct balance for the financial statements.

Control Activities – An element of the COSO internal control framework. Actions, supported by policies and procedures, established and implemented to reduce risk and provide reasonable assurance that specific entity objectives are met. Control activities occur throughout an entity at all levels, and in all functions. They include (1) authorization, (2) review and approval, (3) verification, (4) reconciliation, (5) physical security over assets, (6) segregation of duties, (7) education, training, and coaching, and (8) performance planning and evaluation.

Control Categories – Controls can be categorized as to purpose and when they occur in the transaction cycle.

- A *Preventive control*, q.v., deters the occurrence of undesired events.
- A *Detective control*, q.v., reveals the occurrence of undesired events
- A *Corrective controls*, q.v., remedies the effects of undesired events.

Control Environment – An element of the COSO internal control framework. The entity’s “corporate culture,” showing how much the entity’s leaders value ethical behavior and internal control. It is the control consciousness of an organization and the atmosphere in which people in that organization conduct their activities and fulfill their responsibilities. Factors include:

- Values stated and promoted for integrity and ethical behavior
- Management philosophy and operating style
- Direct and active involvement of the agency management team
- Commitment to competence
- Organization structure
- Assignment of authority and responsibility
- Human Resource policies and practices
- Internal control philosophy
- Risk Management philosophy
- Oversight by control agencies
- Oversight by the agency’s governing board or commission (where applicable)

Control Framework - A control framework is a set of fundamental controls that must be in place to mitigate organizational risk and reduce the likelihood of loss. The most familiar and used of the control frameworks are those promulgated by COSO and ISACA. COSO’s original and now nearly universal internal control frame consisted of five *Components*, q.v., while its newer, expanded version contains eight. ISACA produced COBIT,

GLOSSARY - Consolidated

Control Objectives - Goals or targets to be achieved for each internal control. Objectives should be tailored to fit the specific operations in each entity. The objectives of internal control include the determinations that:

- Transactions are:
 - Valid
 - Accurate
 - Complete
 - Properly authorized
 - Properly valued
 - Properly classified
 - Properly dated and attributed to the correct period
 - Properly posted
 - Properly summarized
 - Recorded at the proper time
- Physical safeguards are adequate
- Proper security is in place
- Error handling is timely and appropriate
- Segregation of duties is maintained
- Programs are managed in accordance with sound business practices

Corrective Control - Controls designed correct previously detected errors or irregularities. The identification of such errors or irregularities and the understanding of how they occurred can at time be used by management in the design of preventive and detective controls.

COSO - The Committee of Sponsoring Organizations of the Treadway Commission, created in 1985. COSO developed the internal control framework that, in one form or another, virtually all organizations currently use.

COSO Component – An element of either the original COSO or updated COSO-ERM internal control frameworks. Also referred to as an internal control component. The original COSO model contains five components: (1) Control Environment; (2) Risk Assessment; (3) Control Activities; (4) Information & Communication; and, (5) Monitoring. The updated COSO-ERM is expanded to include eight components: (1) Internal Environment; (2) Objective Setting; (3) Event Identification; (4) Risk Assessment; (5) Risk Response; (6) Control Activities; (7) Information and Communication; and, (8) Monitoring. Both frameworks are commonly used to identify, evaluate and categorize control weaknesses in organizations.

COSO-ERM – COSO-Environment Risk Management. An updated and expanded version of the original COSO Internal Control Framework. Refer to *COSO Component* for more a more details.

COSO Internal Control Framework – A set of guidelines, developed by COSO, to be used by organizations in establishing and maintaining internal controls. See *COSO Component*.

GLOSSARY - Consolidated

Criteria – In general sense, the standards against which a management control system can be measured in determining effectiveness. The internal control components, taken in the context of inherent limitations of internal control, represent criteria for internal control effectiveness for each of the three control categories. When used in the context of auditing, criteria, one of the elements of an auditor's finding, are what the operation was supposed to accomplish or the conditions that should have existed.

Debarment – The action taken by a government entity to restrict or prohibit future business with an organization or individual.

Deficiency - A perceived, potential, or real internal control shortcoming; or an opportunity to strengthen the management control system, to provide a greater likelihood the entity's objectives are achieved.

Design – (1) Intent. As used in the definition of internal control, management control systems are designed to provide reasonable assurance as to achievement of objectives--when the intent is realized, the system can be deemed effective. (2) Plan. The way a system is supposed to work, contrasted with how it actually works.

Detective Control - A control designed to discover an unintended event or result. Detective controls, as distinct from preventive controls, provide evidence that an error or irregularity has occurred but do not prevent the error or irregularity from occurring.

EDP – Electronic Data Processing. The software and hardware comprising an IT system or the procedures and practices relating to the IT system.

Effective Control - The state or condition of internal control within an entity's management control system in which management (as well as any other governing body) has reasonable assurance of the following:

- management understands the extent to which the entity's operational objectives are being achieved
- organizational resources are being used responsibly
- compliance with applicable laws and regulations is enforced

Effective Management Control System - A synonym for *Effective Control*.

Enterprise Risk Management (ERM) - A process, effected by an entity's directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

Entity - An organization of any size, established for a particular purpose. A governmental entity may be, for example, a state, an agency, a division, a department, or a work unit. In higher education, an entity may be a college, a department, or an administrative unit.

Entity-level Evaluation - An evaluation of an entity, based at least in part on conclusions drawn from *activity-level evaluations*.

GLOSSARY - Consolidated

Ethical Values - Moral criteria enabling a decision maker to determine an appropriate course of behavior. These values should be based on what is "right," and may go beyond what is "legal."

Event Cycle - Processes used to initiate and perform related activities to create the necessary documentation and to gather and report related data (e.g., accounts payable cycle).

Event Identification – A COSO Component. Internal and external events affecting achievement of an entity's objectives must be identified, distinguishing between risks and opportunities. Opportunities are channeled back to management's strategy or objective-setting processes.

Financial Reporting - Used with "objectives" or "controls"—having to do with reliability of published financial statements.

GAAP - "Generally Accepted Accounting Principles" promulgated by the Governmental Accounting Standards Board (GASB) and other standards-setting entities.

General Controls (Information Technology) - Policies and procedures to help ensure the continued, proper operation of computer information systems. General controls include controls over data center operations, system software acquisition and maintenance, access security, and application system development and maintenance. General controls support the functioning of programmed application controls. Other terms sometimes used to describe general controls are general computer controls and information technology controls.

General Controls (Organization) – Practices that broadly support the general control environment of an entity. These include such commonly prescribed safeguards as:

- Segregation of duties
- Use of pre-numbered checks, invoices, vouchers, etc.
- Appropriately securing cash and check stocks
- Limiting the number of authorized signers of checks, purchase orders, etc.
- Limiting access to cash, checks, sensitive or confidential information
- Requiring payment from invoices rather than statements
- Timely third-party review of transactions
- Timely reconciliation of accounts
- Requiring multiple signatures on checks, purchase orders, etc.

General Control Environment - Various factors that can influence the effectiveness of internal controls over program and administrative functions such as an excessive use of a petty cash fund due to heavy travel requirements, which may result in bypassing internal controls. This includes the integrity, ethical values, and competence of an entity's employees, management's philosophy and operating style, organization structure, delegation of authority and responsibility, and written policies and procedures.

Governance – To control, direct, or strongly influence actions or conduct. To exercise power and authority in controlling.

Imprest – A fund, account or cache of money of a fixed amount. Expenditures from an imprest fund will be periodically replenished to maintain the fund's fixed balance.

Imprest Funds – See *Petty Cash*.

GLOSSARY - Consolidated

Information and Communication – An element of the COSO internal control framework. Communicating relevant information in a timeframe to enable people to carry out their responsibilities is an important component of internal control. Effective communication flows in all directions of an entity. An effective information and communication process ensures that all personnel receive a clear message from the head of the entity that internal control must be taken seriously. Information and communication includes a organization's policies and procedures as well as its records of actual events.

Information Technology – A term that encompasses computer systems, their hardware and software components, and the processes that support them. IT concerns itself with automating processes, compiling and distributing information, connecting users, and developing productivity tools.

Inherent Limitations - Limitations applicable to all internal controls within a management control system. The limitations of human judgment; resource constraints and the need to consider the cost of controls in relation to expected benefits; the reality that breakdowns can occur; and the possibilities of management override and of collusion.

Inherent Risk - Degree to which things or activities are exposed to the potential for financial loss, inappropriate disclosure or other erroneous conditions or the risk that one or more factors will prevent an objective from being accomplished, if the entity does not implement risk mitigation measures. For example, activities conducted within severe time constraints have greater inherent risk than those that are not subject to time constraints and cash is more susceptible to misappropriation than large, tangible assets.

Integrity – When applied to persons, the quality or state of being of sound moral principle; uprightness, honesty, and sincerity; the desire to do the "right" thing; and to profess and live up to a set of values and expectations. When applied to things, such as systems, the quality of being complete, sound or unimpaired.

Internal Control – The policies, guidance, instructions, regulations, procedures and other methods designed to provide reasonable assurance regarding achievement of objectives and to mitigate risks in the following categories:

- effectiveness and efficiency of operations
- reliability of financial reporting
- compliance with applicable laws and regulations

Internal Control Components – See *COSO Component*.

Internal Control Concepts - Fundamental concepts of internal control are:

- Internal control is a process – a means to an end, not an end to itself.
- Internal control is affected by people. It is not merely policy manuals and forms, but people at every level of the organization.
- Internal controls are expected to provide only reasonable assurance, not absolute assurance, to an entity's management.
- Internal control focuses on the achievement of objectives in one or more separate but overlapping categories.

GLOSSARY - Consolidated

Internal Control Review - Examination of an entity or operating system to determine whether adequate internal control procedures exist and are effectively implemented to prevent or detect the occurrence of potential risks in a cost-effective manner.

Internal Control System - A synonym for *Internal Control*. Comprises the plan of organization and all methods and procedures adopted by an entity to safeguard its assets, check the accuracy and reliability of its accounting data, promote operational efficiency, and encourage adherence to prescribed managerial policies. Internal control systems include both internal accounting and administrative controls. These two elements of internal control often overlap; however, it is not the intent of this policy to specifically address internal administrative controls.

- Internal accounting controls encompass the plan of organization and all procedures and records that are designed to provide reasonable assurance that:
 - Obligations and costs are in compliance with applicable laws, regulations and policies;
 - Funds, property and other assets are safeguarded against waste, loss, unauthorized use or misappropriation; and
 - All asset, liability, equity, revenue, expenditure/expense and budgetary transactions are properly authorized, recorded, and accounted for to permit the preparation of accurate accounts and reliable financial and statistical reports and to maintain accountability over assets.
- Administrative controls encompass all operational controls within an agency. Their purpose is to insure that agency objectives are met economically, efficiently and effectively, to assure adherence to applicable laws, regulations and policies; and that reliable information is maintained for evaluating managerial and organizational performance to promote operational efficiency.

Internal Environment – A COSO Component. Encompasses the tone of an entity (often referred to as the “tone at the top”), and sets the basis for how risk is viewed and addressed by an entity’s staff, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.

ISACA – Information Systems Audit and Control Association. An organization that focuses on IT governance and control. Its internal control framework is known as COBIT.

IT – See *Information Technology*.

Management – The collective body of those who manage or direct an enterprise.

Management Control System - A set of policies, procedures, and management philosophies, designed to assist management in achieving the strategic objectives of its particular or entity. When a management control system satisfies specific criteria in achieving strategic objectives, it can be deemed effective.

Management Controls - Controls performed by one or more managers at any level in an entity.

Management Intervention – See *Management Override*.

GLOSSARY - Consolidated

Management Override - Management's overruling of prescribed policies, procedures or controls. Management override may occur for legitimate or illegitimate purposes. When undertaken for legitimate purposes, it is sometimes referred to as management intervention. Legitimate purposes include dealing deal with non-recurring or non-standard transactions that might otherwise be incorrectly handled. Illegitimate purposes include both those actions that attempt to achieve illicit personal gain at the expense of the organization and those that misrepresent an entity's financial condition or compliance.

Management Oversight - More than any other individual, the agency head sets the "tone at the top" that affects integrity and ethics and other factors of a positive control environment. In a large entity, the agency head fulfills this duty by providing leadership and direction to senior managers and reviewing the way they are controlling the business. Senior managers, in turn, assign responsibility for establishment of more specific internal control policies and procedures to personnel responsible for the unit's functions. In a smaller entity, the influence of the agency head, often acting as a manager, is usually more direct. In any event, in a cascade of responsibility, a manager is effectively the head of his or her sphere of responsibility. Of particular significance are financial officers and their staffs, whose control activities flow in all directions of the operating and other units of an entity.

Management Process - The series of actions taken by management to run an entity. A management control system is a part of and integrated with the management process.

Manual Controls - Controls performed manually, rather than by computer (contrast with *Computer Controls*).

Master File - A file containing relatively permanent information about the entity or activity to which it pertains. Data elements such as names, addresses, phone numbers, tax rates and the like are generally contained in a master file. Data relating to individual transactions, such as invoice numbers, check amounts, etc., by contrast, are not contained in a master file.

Merchant Fees - Fees associated with a purchase by credit card.

Monitoring – An element of the COSO internal control framework. Monitoring is the assessment of internal control performance over time; it is accomplished by both ongoing monitoring activities and periodic evaluations (i.e., self-assessments, peer reviews, internal audits, etc.)

Objective – Something an organization is legitimately trying to accomplish or attain.

Objective Category - One of four groupings of objectives an entity strives to achieve. The categories are: Strategic – high-level goals aligned with and supporting its mission; Operations - effective and efficient use of resources; Reporting - reliability of reporting; and Compliance – compliance with applicable laws and regulations. The categories overlap, so any one particular objective might fall into more than one category.

Objective Setting – A COSO Component. Objectives must exist before management can identify potential events affecting their achievement. Enterprise risk management ensures that management has in place a process to set objectives and that the chosen objectives support and align with the entity's mission and are consistent with its risk appetite.

GLOSSARY - Consolidated

OMB Circulars - Instructions or information issued by the Office of Management and Budget (OMB) to federal agencies. They are expected to have a continuing effect of two years or more. A complete list of current OMB Circulars can be found on the White House website at <http://www.whitehouse.gov/omb/circulars/>.

Operations - Used with *objectives* or *controls*—having to do with the effectiveness and efficiency of an entity's programs or activities.

PCI - The payment card industry (PCI) denotes the debit, credit, prepaid, e-purse, ATM, and point-of-sale (POS) cards and associated businesses. The term is sometimes more specifically used to refer to the Payment Card Industry Security Standards Council, an independent council originally formed by American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International on Sept. 7, 2006, with the goal of managing the ongoing evolution of the Payment Card Industry Data Security Standard.

Petty Cash - A current asset account that represents an amount of cash for making small disbursements such as postage due and reimbursements for small amounts of supplies. See *Imprest Funds*.

Policy - Management's directive as to what should be done to effect control. A policy serves as the basis for procedures for its implementation.

Pooled Cash - Consists of funds deposited by the individual agencies with the pooled cash accounts of the State Treasurer. Because it is immediately available to the funds, it is considered a form of cash equivalent.

Preventive Control - A control designed to avoid an unintended event or result (contrast with *Detective Control*). Preventive controls proactively attempt to prevent loss. Preventive controls include control activities such as segregation of duties and proper authorization of transactions.

Procedure - An action to implement a policy.

Process - A series of logically related tasks, involving people, machines, and methods; used to change materials, resources, or data (input) into a specified product or service (output).

Program Controls - Controls surrounding the planning and accomplishing of the entity's programmatic goals and objectives. These represent a further level of detail of administrative controls. Examples of program controls are:

- Routine evaluations of the entity's goals, objectives and activities and the extent to which overall objectives are met, and
- Evaluation of how the entity operates to meet their objectives.

Program Objectives - Specific goals, intended changes and desired outcomes of an entity's program activities that can be evaluated and measured.

Public Work - A public work is a construction or engineering project carried out by the government on behalf of the public. Public works include both infrastructure assets (such as airports, canals, dams, dikes, pipelines, railroads, roads, tunnels, and artificial harbors) and non-infrastructure assets (such as mines, schools, hospitals, water purification and sewage treatment centers).

GLOSSARY - Consolidated

Public Use – In a broad and non-legalistic context, the fairly unrestricted access to a facility by the populace. In a narrow, legalistic context, the right of the public to access or benefit from property condemned by the government through the exercise of eminent domain..

Published Financial Statements - Financial statements, interim and condensed financial statements, and selected data derived from such statements (such as monthly budgetary status reports), reported publicly.

Reasonable Assurance - The concept that internal control, no matter how well designed and operated, cannot guarantee an entity's objectives will be met--because *inherent limitations* exist in all management control systems. Reasonable assurance represents a judgment, based upon an evaluation of available information, that an organization's systems of internal control are operating effectively.

Recipient (Prime Recipient) – Prime recipients, also known as “recipients,” are non-Federal entities that receive the proceeds of federal awards directly from the Federal Government.

Reconciliation - An accounting process used to compare two sets of records to ensure the figures are in agreement and are accurate. Reconciliation is the key process used to determine whether the money leaving an account matches the amount spent, ensuring that the two values are balanced at the end of the recording period.

Reliability of Reporting - Used in the context of published financial statements, reliability is defined as the preparation of financial statements fairly presented in conformity with generally accepted (or other relevant and appropriate) accounting principles and regulatory requirements for external purpose, within the context of materiality. Supporting fair presentation are the five basic financial statement assertions, as follows:

- existence or occurrence
- completeness
- rights and obligations
- valuation or allocation
- presentation and disclosure

When applied to interim or condensed financial statements or to select data derived from such statements, both the *factors representing fair presentation* and the *assertions* apply only to the extent they are relevant to the presentation.

Reportable Conditions - An internal control deficiency related to financial reporting—a significant deficiency in the design or operation of the management control system. The deficiency could adversely affect the entity's ability to record, process, summarize, and report financial data consistent with the management's *assertions* in the financial statements.

Residual Risk - The risk that remains after management responds to inherent risk. Once risk responses have been developed, management then considers residual risk.

Response to Risk – See *Risk Response*.

A complete response to a given risk may include more than one alternative.

GLOSSARY - Consolidated

Risk – Anything that could jeopardize the achievement of an objective.

Risk Assessment – An element of the COSO internal control framework. Risk assessment is the identification and analysis of risks associated with the achievement of operations, financial reporting, and compliance goals and objectives. Risk assessment involves analyzing potential events and determining their likelihood of occurrence and their impact on achieving agency objectives. Risk assessment forms a basis for determining an entity's responses to risk.

Risk Identification - A risk is a factor that could prevent an individual, group, or entity from accomplishing an objective as intended or planned. Risk identification encompasses the activities to recognize, discover and categorize the risks pertinent to an organization. It is an element of an organization's risk assessment.

Risk Response – A COSO Component. The set of alternatives used to manage, reduce or tolerate a risk and its potential impact:

- Avoid risk – exit the activities that cause the risk.
- Reduce risk – mitigate the likelihood or negative impact of risk.
- Share risk – assign a portion of risk's impact to another, e.g., through insurance.
- Accept risk – take no action to affect the impact or likelihood of risk.

Segregation of Duties – The concept and practice of having more than one person required to complete a task.

Sight Drafts - A draft or bill that is payable on demand or upon presentation. Also called demand draft. Money is payable at sight, or when the completed documents are presented, or within a specified period called days of grace.

Strategic – Used with objectives; having to do with high-level goals that are aligned with and support the entity's mission (or vision).

Sub-recipient – Sub-recipients are non-Federal entities that are awarded funding through a legal instrument from a Prime Recipient.

Subsidiary ledgers – A group of similar accounts, such as accounts receivable or accounts payable, whose combined balance equals the total for that group of accounts in the general ledger. Subsidiary ledgers contain the details that support the *Control Account* in the general ledger.

Warrants - Warrants are, in effect, checks issued by government entities. Warrants are issued for payroll to individuals and for accounts payable to vendors. Legally, a warrant is a promise to pay when there are sufficient funds in the government's treasury to do so, while a check is a demand draft.

Work Process - A synonym for *Process*.