Statewide Internal Control Guidance

Section: Control Activities

Issued Date: 08/01/2016

Revision Date: 04/01/2022

Index

Overview

Control activities are the actions management establishes through policies and procedures to achieve objectives and respond to risks (including fraud risks) in the internal control system. An organization's internal control system is flexible to allow management to tailor control activities to meet the organization's special needs. The specific control activities used by a given organization may be different from those used by others due to a number of factors. These factors include such things as specific threats the organization faces and risks it incurs, differences in objectives, managerial judgment, size and complexity of the organization, operational environment, sensitivity and value of data, and requirements for information system reliability, availability and performance.

Component	Principles	Attributes
Control Activities	10. Management designs control activities to achieve objectives and respond to risks.	10.1 Response to Objectives and Risks
		10.2 Design of Appropriate Types of Control Activities
		10.3 Design of Control Activities at Various Levels
		10.4 Segregation of Duties
	11. Management designs the information system and related control activities to achieve objectives and respond to risks.	11.1 Design of the Information System
		11.2 Design of the Appropriate Types of Control Activities
		11.3 Design of Information Technology Infrastructure
		11.4 Design of Security Management
		11.5 Design of Information Technology Acquisition, Development, and Maintenance
	12. Management implements control activities through policies.	12.1 Documentation of Responsibilities through Policies
		12.2 Periodic Review of Control Activities

10. Management designs control activities to achieve objectives and respond to risks.

10.1. Response to Objectives and Risks

Concept

Control activities are the policies, procedures, techniques and mechanisms that enforce management's directives to achieve the organization's objectives and address related risks (including fraud risks).

Management Responsibilities

Management designs control activities in order to:

- Fulfill responsibilities defined during the control environment component.
- Address risk responses (including fraud risks) identified during the risk assessment component.

Key Importance to Internal Control

Control activities are needed as a response to the organization's objectives and risks to achieve an effective internal control system.

Example[1]

Management designs control activities to achieve the objectives and address risks (including fraud risks). Some possible ways to do this could include:

- Listing needed responsibilities defined during the control environment phase and brainstorming control activities that would fulfill these responsibilities.
- Listing needed risk responses identified during the risk assessment phase and brainstorming control activities that would provide the needed response.
- Using a top-down, risk-based approach, and identifying the "right combination of controls".
- Applying varying design efforts to risk areas, such as applying increased levels to higher risk areas.

10.2. Design of Appropriate Types of Control Activities

Concept

- Control activities help management fulfill responsibilities and address identified risk responses in the internal control system.
- Control activities can be either preventive or detective, with the main difference being the timing:
  - Preventive – prevents errors from occurring, and preventing these errors helps an organization achieve an objective or addresses a risk.
  - Detective – detects errors or irregularities after it occurs. Also, detective controls discover when an organization is not achieving an objective or addressing a risk and corrects the actions before the organization's operation has concluded so that the organization can achieve the objective or address the risk.

[1] The examples provided throughout this framework are intended to be a minimum starting point and not an all-inclusive list.

- Control activities can be implemented in either an automated or manual manner:
  - Automated – control activities are either wholly or partially automated through the organization's information technology. Automated control activities tend to be more reliable because they are less susceptible to human error and are typically more efficient.
  - Manual – control activities are performed by individuals with minor use of the organization's information technology.

Management Responsibilities

- Management designs appropriate types of control activities for the organization's internal control system.
- Management evaluates the purpose of the control activity as well as the effect a deficiency would have on the organization in achieving their objectives.
  - If the control activity is for a significant purpose, or the impact of a deficiency would be significant, management designs both preventive and detective control activities.
- If the organization relies on information technology in its operations, then management designs control activities so that the information technology continues to operate properly.

Key Importance to Internal Control

Appropriate control activities support an adequate internal control system and allows the organization to achieve their defined objectives.

Example[1]

Management establishes control activities specific to their organization, which could include:

- Control activities in these common categories (see Appendix A for additional details)
  - Segregation of duties.
  - Accurate and timely recording of transactions.
  - Proper execution of transactions.
  - Reconciliations.
  - Controls over information processing.
  - Physical controls over vulnerable assets.
  - Access restrictions to and accountability for resources and records.
  - Appropriate documentation of transactions and internal controls.
  - Establishment and review of performance measures and indicators.
  - Reviews by management at the functional or activity level.
  - Top-level reviews of actual performance.
  - Management of personnel.
- Preventive controls in the above categories, such as:
  - Requiring multiple levels of approval for a transaction.
  - Restricting access.

[1] The examples provided throughout this framework are intended to be a minimum starting point and not an all-inclusive list.

- Detective controls in the above categories, such as:
  - Review of Reports.
  - Bank reconciliations.
- Automated controls in the above categories, such as:
  - Automated validity and edit checks.
  - Sequential pre-numbering of documents.
  - Logical access security (controls who has the ability to read, write, or execute records or data contained in the information system).
- Manual controls in the above categories, such as:
  - Independent review.
  - Exception monitoring.
  - Reconciliations.

10.3. Design of Control Activities at Various Levels

Concept

- Entity-level controls:
  - Have a pervasive effect on an organization's internal control system.
  - May pertain to multiple components.
- Transaction control activities are:
  - Actions built directly into operational processes[2] to support the organization in achieving their objectives or addressing related risks (including fraud risks). "Transactions" [3] tends to be associated with financial processes (payables transactions), while "activities" is more generally applied to operational or compliance processes.

Management Responsibilities

- Management designs control activities at the appropriate levels in the organizational structure.
  - Management designs entity-level control activities, transaction control activities, or both depending on the level of accuracy needed so that the organization meets their objectives and addresses related risks (including fraud risks).
- When choosing between entity-level and transaction control activities, management evaluates the level of accuracy needed for the operational processes, and considers the following:
  - Purpose of the control activity – a control activity that prevents or detects generally is more precise than a control activity that identifies and explains differences.
  - Level of aggregation – a control activity that is performed at a lower level generally is more precise than one performed at a higher level. For example, an analysis of obligations by funding source within the program normally is more precise than an analysis of total obligations for the organization.
  - Consistency of performance – a control activity that is performed routinely and consistently generally is more precise than one performed sporadically.

[2] Operational processes transform inputs into outputs to achieve the organization's objectives.
[3] For this guidance, "transactions" covers both definitions.

- Correlation to relevant operational processes – a control activity that is directly related to an operational process generally is more likely to prevent or detect than a control activity that is only indirectly related.

- Management also is responsible to understand control activities in place when service organizations (third parties) are performing key internal control responsibilities. These third parties could be internal to the State such as GTA (GETS) and SAO (Teamworks or Shared Services) or external such as benefit processing done by a third party.

Key Importance to Internal Control

Control activities designed at the appropriate levels provide appropriate coverage of objectives and identified risks in the operations.

Examples[1]

- Management designs a variety of control activities for operational processes, which could include:
  - Entity- level controls – which may include controls related to the organization's risk assessment process, control environment, service organizations (third parties), management override, and monitoring.
  - Transaction level controls for operational processes – which may include verifications, reconciliations, authorizations and approvals, physical control activities and supervisory control activities.
- Management designs necessary control activities for operational processes (see Appendix A for more details), considering:
  - Who performs the control activity.
  - What is the control activity (not the process).
  - When is the control activity performed.
  - How is the control activity documented.
- Management designs a variety of methods to gain an understanding of control activities for services provided outside of the organization such as:
  - Listing all services not provided internally.
  - Testing of the service organizations (third parties)[4] internal control system.
  - Obtaining a report on controls at the service organization (such as a SOC[5] report).

10.4. Segregation of Duties

Concept

Segregation of duties is designing control activity responsibilities so that incompatible duties are separated and, where such separation is not practical, alternative control activities are designed to address the risk.

[1] The examples provided throughout this framework are intended to be a minimum starting point and not an all-inclusive list.

[4] The service organization (third party) should prepare a description of all applicable controls with sufficient detail for the user agency to plan its own control approach, i.e., help the user agency determine what controls can be relied upon and what controls need to be independently tested.

[5] SOC (System and Organization Controls) reports are internal control reports on the services provided by a service organization providing valuable information that users need to assess and address the risks associated with an outsourced service.

Management Responsibilities

- Management considers the need to separate control activity responsibilities related to authority, custody, and accounting of operations to achieve adequate segregation of duties.
- If segregation of duties is not practical because of limited personnel or other factors, management designs alternative control activities to address the risk of fraud, waste, or abuse in the operational process.

Key Importance to Internal Control

Segregation of duties helps prevent fraud, waste, and abuse in the internal control system. In particular, segregation of duties can address the risk of management override (circumvention of existing control activities) which increases fraud risk, but cannot absolutely prevent it because of the risk of collusion (two or more employees act together to commit fraud).

Examples[1]

- Management designs control activities so not one individual controls all aspects of a cycle. Some possible ways to do this could include:
  - Having someone approve or perform the transaction.
  - Having a different person record the transaction.
  - Having a different person prepare applicable reconciliations relating to the transaction.
  - Having a different person prepare the report relating to the transaction.
- Management designs mitigating control activities if segregation of duties is not possible. Some possible ways to do this could include:
  - Having someone perform, record, reconcile and report the transaction.
  - Having a different person verify the work performed by the first person.
  - Having increased review or supervision by management.

11. Management designs the information system and related control activities to achieve objectives and respond to risks.

11.1. Design of the Information System

Concept

- An information system:
  - Is the people, processes, data and technology that management organizes to obtain, communicate, or dispose of information.
  - Represents the life cycle of information used for the operational processes that enables the organization to obtain, store, and process quality information.
  - Includes both manual and technology-enabled information processes.

[1] The examples provided throughout this framework are intended to be a minimum starting point and not an all-inclusive list.

- Technology-enabled information processes are commonly referred to as information technology, which:
  - Enables information related to operational processes to become available on a timelier basis.
  - May enhance internal controls over security and confidentiality of information by appropriately restricting access.
- Information technology implies specific types of control activities but it is not a stand-alone control consideration. Instead, information technology is an integral part of most control activities.

Management Responsibilities

- Management designs the organization's information system and the use of information technology by considering the information requirements for each of the organization's operational processes.
- Management evaluates information processing objectives to meet the defined information requirements, these objectives include the following:
  - Completeness – transactions that occur are recorded and not understated.
  - Accuracy – transactions are recorded on a timely basis, at the correct amount, and in the right account at each stage of processing.
  - Validity – recorded transactions represent events that actually occurred and were performed according to prescribed procedures.
- Management designs control activities, for the organization's information system, to fulfill responsibilities defined during the control environment component and address risk responses (including fraud risks) identified during the risk assessment component.

Key Importance to Internal Control

Properly designing the organization's information system will help enhance internal control over security and confidentiality of information, and enable the organization to achieve their objectives and respond to identified risks.

Example[1]

Management designs the information system to achieve the objectives and address risks (including fraud risks). Some possible ways to do this could include:

- Listing needed information requirements and brainstorming the information system that would fulfill these requirements.
- Using pre-established accounting software (such as Teamworks).
- Contracting with someone more specialized, such as GTA.

11.2. Design of the Appropriate Types of Control Activities

Concept

Control activities are the policies, procedures, techniques and mechanisms that enforce management's directives to achieve the organization's objectives and address related risks (including fraud risks).

[1] The examples provided throughout this framework are intended to be a minimum starting point and not an all-inclusive list.

Management Responsibilities

Management designs appropriate types of control activities (in the information system) for coverage of information processing objectives relating to operational processes. For the information system, there are two main types of control activities, general and application control activities:

- General controls – can be at the entity-wide, system, and application levels, and:
  - Are the policies and procedures that apply to all or a large segment of an organization's information systems.
  - Facilitate the proper operation of the information systems by creating the environment for proper operation of application controls.
- Application controls – are sometimes referred to as business process controls, and are those controls that are incorporated directly into computer applications to achieve:
  - Validity, completeness, accuracy, and confidentiality of transactions and data during application processing.

Key Importance to Internal Control

Controls activities in the organization's information systems provide coverage for the information processing objectives which eventually help to achieve an effective internal control system.

Example[1]

Management designs control activities considering the need for general and application controls:

- General controls, with some possibilities including:
  - Security management.
  - Logical and physical access.
  - Configuration management.
  - Segregation of duties.
  - Contingency planning.
- Application controls, which includes controls over:
  - Input.
  - Processing.
  - Output.
  - Master file.
  - Interface.
  - Data management controls.

[1] The examples provided throughout this framework are intended to be a minimum starting point and not an all-inclusive list.

11.3. Design of Information Technology Infrastructure

Concept

Information technology infrastructure:

- Can be complex.
- Includes communication networks for linking information technologies, computing resources for applications to operate, and electricity to power the information technology.
- May be shared by different operating division/programs within the organization or outsourced either to service organizations (third parties) or to location-independent technology services.

Management Responsibilities

- Management evaluates the objectives of the organization and related risks (including fraud risks) in designing control activities for the information technology infrastructure.
- Management designs control activities over the information technology infrastructure to support the completeness, accuracy, and validity of information processing and to maintain the information technology infrastructure.
- Management continues to evaluate changes in the use of information technology and designs new control activities when these changes are incorporated into the organization's information technology infrastructure.

Key Importance to Internal Control

Control activities over the information technology infrastructure support the completeness, accuracy, and validity of information processed, which helps to strengthen the internal control system, and aids the organization in achieving their objectives and addressing identified risks.

Example[1]

Management designs the information technology infrastructure by considering needs, such as:

- Communication networks for linking information technologies
- Computing resources for applications to operate.
- Electricity to power the information technology.
- Backup and recovery procedures along with continuity of operation plans, depending on the risks and consequences of a full or partial systems outage.

11.4. Design of Security Management

Concept

- Security management includes the information processes and control activities related to access rights in an organization's information technology, including who has the ability to execute transactions. This would include access rights across various levels of data, the operating system, the network, applications, and physical layers.

[1] The examples provided throughout this framework are intended to be a minimum starting point and not an all-inclusive list.

- Objectives for security management include:
  - Confidentiality – data, reports, and other outputs are safeguarded against unauthorized access.
  - Integrity – information is safeguarded against improper modification or destruction, which includes ensuring the information's origin and authenticity.
  - Availability – data, reports, and other relevant information are readily available to users when needed.

Management Responsibilities

- Management evaluates security threats to information technology, which can be from both internal and external sources:
  - Internal threats – may come from former or disgruntled employees. They pose unique risks because they may be both motivated to work against the organization and better equipped to succeed in carrying out a malicious act as they have greater access to and knowledge of the organization's security management systems and processes.
  - External threats – particularly important for entities that depend on telecommunications networks and the Internet. External threats have become prevalent in today's highly interconnected business environments, and continual effort is required to address these risks.
- Management designs control activities for security management that:
  - Allows for appropriate access by internal and external sources to protect the organization's information system from inappropriate access and unauthorized use of the system.
  - Contains access rights when different information technology elements are connected to each other.
  - Supports appropriate segregation of duties by restricting access to applications or functions.

Key Importance to Internal Control

By preventing unauthorized use of and changes to the system, data and program integrity are protected from error or malicious intent (e.g., someone breaking into the technology to commit fraud, vandalism, or terrorism).

Example[1]

Management designs the security management control activities for information technology, (which also includes high risk spreadsheets, databases, and other user developed programs). Some possible ways to do this could include:

- Limiting user access to information technology through authorization controls activities such as providing unique user identification or requiring multiple level authentication.

[1] The examples provided throughout this framework are intended to be a minimum starting point and not an all-inclusive list.

- Restricting authorized users to the applications or functions at a minimum level appropriate for assigned responsibilities, while also supporting an appropriate segregation of duties, such as:
  - Limiting access to specific rights within a particular system, application or to certain files.
  - Restricting the ability to write, delete, or execute within a particular system, application or to certain files.
- Designing other control activities to promptly update access rights when employees change job functions or leave the organization.
- Having version or change control techniques to control access to and modification of systems and files, as well as to track versions and revisions.
- Implementing controls to confirm the data housed in programs or via spreadsheets and databases are complete and accurate.
- Performing backups to make copies of the data that could be restored after a data loss event.

11.5. Design of Information Technology Acquisition, Development, and Maintenance

Concept

A process that outlines specific phases and documentation requirements, approvals, and checkpoints over the acquisition, development, and maintenance of technology. Management may use a systems development life cycle (SDLC) framework in designing control activities. Through a SDLC, management designs control activities over changes to technology, and depending on the size and complexity of the organization, this may be included in one SDLC or two separate methodologies.

Management Responsibilities

- Management designs control activities associated with the:
  - Acquisition, development and maintenance of information technology, and also evaluates the objectives and risks (including fraud risks) of the new technology.
  - Acquisition of vendor packaged software along with the related ongoing development and maintenance.
  - Objectives and related risks (including fraud risks) for an SDLC developed internally.
- Management also evaluates the unique risks (including fraud risks) that outsourcing the development of information technology to a service organization (third party) presents for the completeness, accuracy, and validity of information submitted to and received from the service organization (third party).

Key Importance to Internal Control

Control activities for the development, maintenance, and change of application software prevent unauthorized programs or inappropriate modifications to existing programs or files, which helps to strengthen data within the internal control system.

Example[1]

Management designs the control activities for information technology acquisition, development, and maintenance which could include:

- Requiring authorization of change requests.
- Reviewing the changes, approvals, and testing results.
- Designing protocols to determine whether changes are made properly.

12. Management implements control activities through policies.

12.1. Documentation of Responsibilities through Policies

Concept

The internal control responsibilities of the organization are documented in policies.

Management Responsibilities

- Management documents in policies, at the appropriate level of detail, each division/program's responsibility for the:
  - Objectives and related risks (including fraud risks) of an operational process.
  - Control activity design, implementation, and operating effectiveness.
- Each division/program, with guidance from management:
  - Determines the policies necessary to operate the process based on the objectives and related risks (including fraud risks) for the operational process.
  - Documents the policies in the appropriate level of detail to allow management to effectively monitor the control activity.
- Those in key roles of the division/program may further define policies through day-to-day procedures, depending on the rate of change in the operation environment and complexity of the operational process.
  - Procedures may include the timing of when a control activity occurs and any follow-up corrective actions to be performed by competent personnel if deficiencies are identified.
- Management communicates the policies and procedures so that personnel can implement the control activities for their assigned responsibilities.

Key Importance to Internal Control

Policies document internal control responsibilities so personnel can perform their assigned responsibilities which will help an effective internal control system be implemented.

Example[1]

Management documents the control activities in a variety of methods selecting the most efficient and effective considering the need for future changes, which could include:

- Narratives (describes a process or transaction flow using words rather than a pictorial representation).
- Flowcharts (which is a diagram that shows step-by-step progression generally using connecting lines and a set of conventional symbols).

[1] The examples provided throughout this framework are intended to be a minimum starting point and not an all-inclusive list.

12.2. Periodic Review of Control Activities

Concept

The control activities of the organization are periodically assessed to ensure they are still relevant and effective.

Management Responsibilities

- Management periodically reviews policies, procedures, and related control activities for continued relevance and effectiveness in achieving the organization's objectives or addressing related risks (including fraud risks).
- Management reviews, in a timely manner, an organization's process that had a significant change, to determine that the control activities are still designed and implemented appropriately. Changes may occur in the personnel, operational processes, information technology or in relation to the organization's objectives[6].

Key Importance to Internal Control

The review of control activities to keep them relevant and effective will help maintain the effectiveness of the overall internal control system and allow the organization to achieve their objectives.

Example[1]

Management reviews the control activities in a variety of methods, which could include:

- Having discussions at defined time periods.
- Having a process to identify significant changes and the need for review of control activities.
- Having a reviewer independent of the activity evaluate the design.

[1] The examples provided throughout this framework are intended to be a minimum starting point and not an all-inclusive list.

[6] Regulators, Legislators, and the Governor's Office of Planning and Budget may also change either an organization's objectives or how an organization is to achieve an objective.

Appendix A
Common Categories of Control Activities

This list is not all inclusive and may not be particular control activities that an organization may need:

- Segregation of duties – assigning key duties and responsibilities to different personnel to reduce the risk of error, misuse, or fraud. This includes separating the responsibilities for authorizing, processing and recording, reviewing, and handling any related assets, so that no one individual controls all key aspects of a transaction or event.

- Controls over information processing – using a variety of control activities, such as edit checks of data entered, accounting for transactions in numerical sequences, comparing file totals with control accounts, and controlling access to data, files and programs.

- Accurate and timely recording of transactions – recording transactions promptly in a complete and accurate manner. This applies to the entire process or life cycle (from initiation and authorization through final classification in summary records).

- Proper execution of transactions – authorizing and executing transactions only by persons possessing proper authority, so that only valid transactions to exchange, transfer, use, or commit resources are initiated and entered into. Management clearly communicates this authorization to personnel.

- Reconciliations – comparing balances in the accounting records to source documents (such as cash balances recorded as compared to the bank statement), and following up on any differences. For inventorial items, periodically counting and comparing vulnerable assets (such as cash, securities, inventories, and equipment) to control records.

- Physical controls over vulnerable assets – securing and safeguarding vulnerable assets that have a risk of loss or unauthorized use through physical controls. Examples of physical controls could include security for and limiting access to assets.

- Access restrictions to and accountability for resources and records – limiting access to resources and records to authorized individuals, and assigning and maintaining accountability for their custody and use. Periodically review the recorded custody and usage to help reduce the risk of errors, fraud, misuse, or unauthorized alteration.

- Appropriate documentation of transactions and internal controls – documenting transactions, internal controls, and other significant events clearly, with the records being properly managed, maintained and readily available for examination. The documentation may appear in management directives, administrative policies, or operating manuals, in either paper or electronic form.

- Establishment and review of performance measures and indicators – establishing activities to monitor performance measures and indicators, by assessing different sets of data and taking appropriate actions. Also, designing controls to validate the propriety and integrity of the performance measures and indicators.

- Reviews by management at the functional or activity level – comparing actual performance to planned or expected results and analyzing significant differences.

- Top-level reviews of actual performance – tracking and comparing major organizational achievements to the plans, goals and objectives.

- Management of personnel – managing effectively the organization's workforce:
  - Ensuring the right personnel for the job are on board and are provided the right training, tools, structure, incentives and responsibilities so operational success is possible.
  - Continually assessing the knowledge, skill, and ability needs of the organization to obtain a workforce qualified to achieve organizational goals.
  - Considering retention of valuable employees, planning for their eventual departure and maintaining a continuity of needed skills and abilities.
  - Providing training, supervision and feedback to personnel:
    - Training is aimed at developing and retaining employee knowledge, skills, and abilities to meet changing organizational needs.
    - Continually provide supervision to ensure that internal controls objectives are achieved.
    - Providing performance evaluation and feedback to personnel so they can understand the connection between their performance and the organization's success.