Overview:

Control Activities are the actions established through policies and procedures to help ensure management's directives to mitigate risks to the achievement of objectives are carried out. Control activities are performed at all levels of the entity, at various stages within the business processes, and over the technology environment. They may encompass a range of manual and automated activities such as authorizations and approvals, verifications, reconciliations, and business performance reviews. Control activities can support one or more of the entity's operations, reporting, and compliance objectives.

All staff, not only management, should be aware of the relevance of risk and the importance of controls to the achievement of the objectives. Staff should be trained to support management in reviewing internal controls, noting if they are not working, identifying new risks, and recommending new internal controls to mitigate the new risk.

The third component of the framework is Control Activities.

Control Activities are actions to help ensure responses to assessed risks and other management directives, such as establishing standards of conduct in the control environment, are carried out properly and in a timely manner.

Risks are addressed by four different categories of controls:

- **Preventive Controls** are steps taken before an emergency, loss, or problem occurs. They are designed to limit the possibility of an undesirable outcome being realized. These include use of alarms and locks, segregation of duties, plus other authorization policies. They are designed to focus on preventing errors or exceptions.
- **Detective Controls** are control techniques for early discovery of problems and to quickly correct errors or exceptions after occurring. They are designed to identify occasions of undesirable outcomes having been realized. Examples are asset verifications, reconciliations, financial statement/budget reviews, and periodic review of expenditure reports. They are designed to identify an error or exception after it has occurred.
- **Corrective Controls** are designed to correct a realized, undesirable outcome and to provide recourse to achieve recovery against the loss or damage. Examples are insurance policies and contingency planning. They are designed to reverse the effects of errors detected and fix the issue or exception.
- **Directive Controls** are activities that direct employee behavior. Examples are policy and procedures, law and regulations, training seminars, and job descriptions. They are designed to ensure a particular outcome is achieved.

The critical part of the control activity is the action taken to prevent, detect, correct or avoid an unintended event or result.

The designed internal control should be in proportion to the perceived risk. Management considers the precision of the control activity, that is, how exact it will be in preventing or detection an unintended event or result. Except with critical risks, it is sufficient to design controls to provide reasonable

assurance of confining a loss within the organization's risk appetite. The cost of implementing and maintaining the control should be less than the cost of the loss including a loss in reputation. The purpose of the control is to constrain, rather than eliminate, the risk.

Management may consider layering internal controls to mitigate risk to critical data, information, and processes. Layering means using two or more internal controls to mitigate one risk. Use a preventive control to prevent an identified risk from occurring; a detective control to identify an incident in a timely manner; a corrective control to define the process to correct the incident and to reassess the control activities.

The Control Activities component contains three principles, and to help management and the oversight body to achieve each principle, there are attributes pertaining to each of the three principles.

Principle 10- Design Control Activities:

"Management should design control activities to achieve objectives and respond to risks."

Attributes:

- Response to objectives and risks
- Design of appropriate types of control activities
- Design of control activities at various levels
- Segregation of duties

Response to Objectives and Risks:

Control activities are the policies, procedures, techniques, and mechanisms to enforce management's directives to achieve the entity's objectives and address related risks. To this end, management designs control activities to respond to the objectives and address related risks to achieve an effective internal control system.

Management establishes the control environment by defining responsibilities, assigning them to key roles, and delegating authority to achieve its objectives. Next, management conducts a risk assessment by identifying the risks related to the entity and its objectives, the risk tolerance, and risk responses. Now, management must design control activities to fulfill defined responsibilities and address identified risk responses.

Design of Appropriate Types of Control Activities:

Control activities help management fulfill responsibilities and address identified risk responses through the internal control system at the appropriate levels in the organizational structure.

Each control activity wording should describe how it is designed to mitigate the risk, the likelihood it will be effective, and a method to verify it is functioning as intended.

Many entities use outsourced service providers, a.k.a. third party administrators, contractors, vendors, for software, data processing needs, and other processing needs. While the service is provided outside the entity, the risk responsibility remains with management and should be included in the risk assessment process. When you give a company your personal, customer, financial data, or any access to your systems, you are opening yourself up to potentially expose that data to anyone that uses that third party. When a request for proposal is prepared, management should request information about the vendor's internal controls, either as a statement of controls and their effectiveness for a small business or as a Service Organization Control (SOC) 1 report for a larger organization.

A SOC 1 report is an independent report by an accounting firm focusing on internal controls at the service organization. The SOC 1 report contains a description of the service organization's internal control system and an assertion from management as it pertains to financial reporting. The independent service auditor (i.e., CPA firm) opinion or service auditor report is the body of this report.

There are two types of SOC 1 reports: Type I and Type II. A Type I reports on the fairness of the presentation of management's description of the service organization's internal control system and the suitability of the design of the controls to achieve the related control objectives included in the description as of a specified date. (e.g. June 30, 20xx). A Type II reports on the fairness of the presentation of management's description of the service organization's internal control system and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives included in the description throughout a specified period (e.g. January 1, 20xx to June 30, 20xx).

Design of Control Activities at Various Levels:

Operational processes transform inputs into outputs to achieve the organization's objectives.

When determining what actions to put in place to mitigate risk, management considers all aspects of the entity's internal control components and relevant business processes, information technology, and locations where control activities are needed. This may require considering control activities outside the operating unit, including shared service or data centers, and processes or functions performed by outsourced service providers.

Entity-level controls are controls having a pervasive effect on an entity's internal control system and may pertain to multiple components. These controls are related to the entity's risk assessment process, control environment, service organizations, management override, and monitoring.

Transaction controls are the most fundamental control activities and are selected and developed to be applied to operational and compliance processes. Transaction control activities are actions built directly into operational processes to support the entity in achieving it objectives and addressing related risks.

Controls for operational processes include: verifications, reconciliations, authorizations, approvals, physical control activities, and supervisory control activities.

Segregation of Duties:

Segregation of duties helps to deter fraud, waste, and abuse. Management considers separating control activities related to authority, custody, and accounting of operations to achieve adequate segregation of duties. If this is not practical, management should design alternative control activities to address the risk of fraud, waste, and abuse.

Segregation of duties may address important risks relating to management override. Management override circumvents existing controls and is an often-used means of committing fraud. Segregation of duties reduces, but does not absolutely prevent, the possibility of one person acting alone. Collusion is needed to perform fraudulent activities when key process responsibilities are divided between at least two employees. Segregation of duties reduces errors by having more than one person performing or reviewing transactions in a process, increasing the likelihood of an error being detected and reducing the opportunity for fraud.

Principle 11- Design Activities for the Information System:

"Management should design the entity's information system and related control activities to achieve objectives and respond to risks."

Attributes:

- Design of the entity's information system
- Design of appropriate types of control activities
- Design of information technology infrastructure
- Design of security management
- Design of information technology acquisition, development, and maintenance

Design of the Entity's Information System:

An information system is the people, processes, data, and technology that management organizes to obtain, communicate, or dispose of information. An information system includes both manual and automated technology-enabled information processes. Management designs control activities to fulfill defined responsibilities and address the identified risk responses for the entity's information system.

Information processing objectives may include completeness, accuracy, and validity.

- Completeness means all transactions are recorded.
- Accuracy means transactions are recorded at the correct amount, in the correct account, at the correct time at each stage of the process.
- Validity means transactions represent the event as it actually occurred and was executed according to prescribed procedures.

Restricted access is an important consideration for most business processes and is often included as an information processing objective because without appropriately restricting access over transactions in a

business process, the control activities may be overridden and segregation of duties may not be achieved.

Design of Appropriate Types of Control Activities:

A variety of transaction control activities may be selected and developed, including:

- Authorizations and Approvals – An authorization affirms a transaction is valid (i.e., it represents and actual economic event or is within an entity's policy). An authorization takes the form of an approval by a higher level of management or verification and determination the transaction is valid. For example, a supervisor approves an expense report after reviewing to ensure the expense is reasonable and within policy.
- Verifications – Verifications compare two or more items with each other or compare an item with policy, and perform a follow-up action when the two items do not match or the item is not consistent with policy.
- Physical Controls – Equipment, inventories, securities, cash, and other assets are secured physically (e.g., in locked or guarded storage areas with physical access restricted to authorized personnel) and are periodically counted and compared with amounts shown in control records.
- Controls over Standing Data – Standing data, such as the price master file, is often used to support the processing of transactions within a business process. Control activities over the processes to populate, update, and maintain the accuracy, completeness, and validity of this data are put in place by the organization.
- Reconciliations – Reconciliations compare two or more data elements and if differences are identified, corrective action is taken to bring the data into agreement. Also, procedures should be reviewed to help prevent the error to recur.
- Supervisory Controls – Supervisory controls assess whether other transaction control activities (i.e., particular verifications, reconciliations, authorizations and approvals, controls over standing data, and physical control activities) are being performed completely, accurately, and according to policy and procedures.

When designing and developing control activities, it is important to:

- Understand what a particular control is designed to accomplish (i.e., the specific risk response addressed by the control), and
- Verify the process development and its implementation are functioning together to mitigate the risk.

For information systems, there are two main types of control activities: general and application control activities.

- General controls (at the entity-wide, system, and application levels) are the policies and procedures which apply to an entity's information systems. General controls facilitate the proper operation of information systems by creating the environment for proper operation of application controls. General controls include security management, logical and physical access, configuration management, segregation of duties, and contingency planning.

- Application controls, also known as business process controls, are controls incorporated directly into computer applications to achieve validity, completeness, accuracy, and confidentiality of transactions and data during application processing. Application controls include controls over input, processing, output, master file, interfaces, and data management system controls.

Design of Information Technology Infrastructure:

Control activities and technology are related in two ways:

- Technology supports business processes. When technology is embedded within the entity's business processes, control activities are needed to mitigate the risk the technology itself will not continue to operate properly to support the achievement of the organization's objectives.
- Technology is used to automate control activities. Many control activities are partially or wholly automated using technology.

Information technology requires an infrastructure to operate, including communication networks for linking information technologies, computing resources for applications to operate, and electricity to power the systems.

The system may be shared by different units within the entity or outsourced to service organizations. Management evaluates the objectives of the entity and related risks in designing control activities for the information technology infrastructure. Management also designs control activities needed to maintain the information technology infrastructure, including backup and recovery procedures, and business continuity plans.

Design of Security Management:

Objectives for security management include confidentiality, integrity, and availability.

Confidentiality means that data, reports, and other inputs and outputs are safeguarded against unauthorized access. Integrity means that information is safeguarded against improper modification or destruction, which includes ensuring information's nonrepudiation and authenticity. Availability means that data, reports, and other relevant information are readily available to authorized users when needed.

Security management includes control activities for access rights in an entity's information technology across various levels of data, operating system (system software), network, application, and physical layers.

Management designs control activities over access to protect an entity from inappropriate access and unauthorized use of the system. By preventing unauthorized use of and changes to the system, data and program integrity are protected from malicious intent (e.g., someone breaking into the technology to commit fraud, vandalism, or terrorism) or error.

Management designs control activities to limit user access to information technology through authorization control activities such as providing a unique user identification or token to authorized

users. These control activities may restrict authorized users to the applications or functions commensurate with their assigned responsibilities, supporting an appropriate segregation of duties. Management designs other control activities to promptly update access rights when employees change job functions or leave the entity. Management also designs control activities for access rights when information technology elements are connected to each other.

Design of Information Technology Acquisition, Development, and Maintenance:

A systems development life cycle (SDLC) provides a structure for a new information technology design by outlining specific phases and documenting requirements, approvals, and checkpoints within control activities over the acquisition, development, and maintenance of technology.

This involves requiring authorization of change requests; reviewing the changes, approvals, and testing results; and designing protocols to determine whether changes are made properly. Depending on the size and complexity of the entity, development of information technology and changes to the information technology may be included in one SDLC or separate methodologies. Management evaluates the objectives and risks of the new technology in designing control activities over its SDLC.

An alternative is outsourcing the development of information technology to service organizations. As for an SDLC developed internally, management designs control activities to meet objectives and address related risks. Management also evaluates the unique risks presented by using a service organization to ensure the completeness, accuracy, and validity of information submitted to and received from the service organization.

Principle 12- Implement Control Activity:

"Management should implement control activities through policies."

Attributes:

- Documentation of responsibilities through policies
- Periodic review of control activities

Documentation of Responsibilities Through Policies:

Policies reflect management's statement of what should be done to effect control by written documentation, by explicit communications, or by implication through management's actions and decisions.

Unwritten policies may be effective when the policy is a long-standing and well-understood practice. However, unwritten policies and procedures may be easier to circumvent, be costly when employee turnover is high, and may reduce accountability.

Whether written or not, policies and procedures must establish clear responsibility and accountability which resides with management of the entity and with the subunit where the risk resides.

Management documents in the policies for each unit its responsibility for an operational process's objectives and related risks, and control activity design, implementation, and operating effectiveness.

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. Each unit, with guidance from management, determines the policies necessary to operate the process based on the objectives and related risks for the operational process. Each unit also documents policies in the appropriate level of detail to allow management to effectively monitor the control activity.

Management communicates to personnel the policies and procedures so that personnel can implement the control activities for their assigned responsibilities.

Periodic Review of Control Activities:

Management periodically reviews policies, procedures, and related control activities for continued relevance and effectiveness, unrelated to being responsive to significant changes in the entity's risks or objectives. If there is a significant change in an entity's process, management reviews this process in a timely manner after the change to determine whether the control activities are designed and implemented appropriately. Changes may occur in personnel, operational processes, legislation, or information technology.

Changes in people, process, and technology may reduce the effectiveness of control activities or make some control activities redundant. A well-designed control activity cannot be conducted without competent personnel having sufficient authority to perform it. Furthermore, a procedure performed by rote, without sharp, continuous focus on the risks to which the policy is directed, may overlook a significant incident. Sufficient authority may be needed to fully perform all aspects of the control such as taking corrective action.

QUESTIONS TO CONSIDER WHEN IMPLEMENTING CONTROL ACTIVITIES:

- What type of control is needed – Preventive? Detective? Corrective? Directive? None? Two or more?
- Is this a critical data/process requiring stricter controls?
- Should the control be manual or automated?
- If manual, will it be effective consistently?
- If manual, is it documented to transfer to a new employee?
- If manual, how will I know it is effective?
- If automated, is it designed as requested?
- If automated, is it functioning as intended?
- If automated, is there a reconciliation, notification, or process to determine if it is not working as intended?
- Is one person able to control all steps in a process, for example, place an order for goods, receive the goods, and process payments for those goods?
- If staff is limited, is there a reconciliation process to detect payments for unauthorized goods or services?

- Is it possible for management to override manual or automated controls to the detriment of the organization?
- When an error occurs, is there a procedure to correct it?
- If there is a preventive control, is a detective control also needed?
- Does my service provider have adequate controls to protect my data?
- Could any of my service provider's service providers use their access to access my data or my organization?
- Does my agreement with my service provider contain a clause requiring a SOC 1 Type 1 or Type 2 report on a regular basis?
- Do I understand how my internal controls are intended to function?
- How do I know my internal controls are effective?
- How do I ensure my internal controls are functioning as intended?
- When my personnel changes duties, is access to all systems reviewed to ensure prior accesses are terminated before new accesses are granted?
- When my personnel leave the organization, are all accesses to the facility and all systems terminated promptly?
- Does the edit check to prohibit an employee from approving his own transactions function as intended?
- Does the edit check to ensure a transaction is approved function as intended?
- Have all edit checks been tested to ensure they are functioning as intended, i.e., can alpha characters be entered in a numeric field?
- Are reconciliations performed to ensure all transactions are processed and processed accurately?
- Are reconciliations performed to ensure only approved transactions are processed and processed accurately?
- Are reconciliations performed to ensure processed transactions are valid and properly approved?
- How do I know all of my data is valid?
- Do I understand how the application controls for my transactions were designed to function?
- Do I know if these application controls are functioning as intended?
- Do I know if there are recovery plans in case of a power outage or other incident causing a system failure?
- Do I have a current business continuity plan? Is all contact information current?
- Did I take an active role in designing the new software system to ensure it is functioning as I expected?
- What if all of my policies and procedures are not documented?
- What if all of my policies and procedures are not current?
- Have I considered the controls needed to ensure my policies and procedures are followed?
- When do I review my control activities?
  - Never?
  - When new employees are hired?
  - When employees change roles?
  - When employees leave?
  - When a new system is implemented?
  - When there is a cybersecurity breach?