Internal Control Glossary

Control Environment: sets of standards, processes, structures, and environment established and maintained by management to provide the foundation and basis for carrying out an internal control system cross the organization.

Common Terminology	Description
Tone at the Top	Management leads by example (through directives, attitudes, and behavior) to demonstrate a commitment to the organization's integrity and ethical values.
Standards of Conduct	Management defines and communicates the organization's expectations of ethical values to employees and other related parties through different formats, such as policies, operating principles, guidelines etc. Management also establishes a process for evaluating individual and/or team adherence to the organization's approved Standards of Conduct and takes action when nonconformities occur.
Oversight	Board of Director/Oversight Body who oversees management's design, implementation, and operation of the organization's internal control system.
Organization Structure	Management defines roles and assigns responsibilities at different units or levels of the organization to operate in an efficient and effective manner.
Commitment to Competence	Management establishes expectations of competence on recruiting, developing, and retaining personnel.
Accountability	Personnel's responsibilities, such as day-to-day decision making, attitudes, and behaviors that are enforced by management through performance reviews and/or disciplinary actions.

Internal Control Glossary

Risk Assessment: Involves a dynamic and interactive process for identifying and analyzing risks from both external and internal sources to achieve the organization's objectives. This assessment helps management to determine how risks should be managed.

Common Terminology	Description
Risk	The possibility that error or irregularity will happen to negatively affect the organization to achieve an objective related to operations, reporting, and compliance.
Inherent Risk	The risk to an organization that may lead to potential financial loss, inappropriate disclosure or other erroneous conditions, in the absence of management's response to the risk.
Residual Risk	The risk that remains after management responds to inherent risk.
Fraud Risk	Fraud involves obtaining something of value through willful misrepresentation. Types of fraud include fraudulent financial reporting, misappropriation of assets, and corruption. Incentive/pressure, opportunity, and attitude/rationalization are the primary fraud risk factors.
Risk Identification	A process to recognize, discover, determine and categorize risks that exist or are anticipated relating to the organization's objectives. Objectives should be specific, measurable, attainable, and relevant to enable the identification of risk. Risk can be identified through two types of assessment, quantitative and qualitative risk analysis.
Quantitative Risk Analysis	A numerical based assessment on financial line items amount to determine materiality threshold (refer to GAO Financial Audit Manual for additional guidance).
Qualitative Risk Analysis	A more subjective analysis based on external and internal events. Examples include complexity of process, level of manual intervention, managed by a 3rd party, history of audit issues, changes in laws and regulations, human capital management.
Risk Tolerances	Setting the acceptable level of variation for the organization's objectives. When operating within risk tolerances, management has greater assurance that the organization will achieve its defined objectives.
Risk Responses	Management considers the significance of the identified risks and level of risk tolerances to design responses and take specific actions. Risk responses may include the following: • *Acceptance*: no action due to insignificance of the risk • *Avoidance*: take action to stop the entire or partial process causing the risk • *Reduction*: take action to reduce the possibility/extent of the risk • *Sharing*: take action to transfer or share risks across the organization or with external parties

Internal Control Glossary

Control Activities: Actions directed by management through established policies and procedures to mitigate the identified risks to acceptable levels. These activities are performed at all levels of the organization and at different stages within operation processes (including IT systems).

Common Terminology	Description
Controls	Management's tools (policies, procedures, techniques, mechanisms, etc.) that help identify, prevent or reduce risk that has adverse impact on the organization's objectives.
Control Objective	The goal to be achieved for a control that is designed and implemented for the organization.
Key Control	Control that is designed by management within an operation process to prevent a significant risk to occur.

Type of Control	Definition	Examples
Preventive	Control that helps management to avoid issues before they occur.	• Training • Review and Approval Process • System Access Authorization • Segregation of Duties • Physical Safeguard of Assets
Detective	Control that discover issues after they occur.	• Reconciliation • Trace Transaction to Source Document • Monitor Actual vs. Budget • Review Activity Logs
General (IT)	Policies and procedures that apply to all or a large portion of an organization's information systems that facilitate the proper system operation environment.	• Security Management • Logical and Physical Access • Configuration Management • Segregation of duties • Contingency Planning
Application (IT)	Control that is incorporated into computer applications to ensure validity, completeness, accuracy, and confidentiality of transactions and data during system processing.	• Edit Checks for Input Data • Numerical Sequence Checks • Interface • Data Management System Control

Internal Control Glossary

Information and Communication: Management communicates relevant and timely information to internal and external to support the internal control syste**m.**

To select an appropriate method of communication (internally/externally), management should consider the following factors:

Factor	Description
Audience	The targeted recipients of the information anticipated to be delivered.
Nature of Information	The type of information being communicated.
Availability	The accessibility of information to the audience.
Cost	The amount of resources needed to communicate the information.
Legal or Regulatory Requirements	Requirements in laws/regulations that can impact the communication.

Monitoring: Management performs ongoing evaluations and/or separate evaluations to ensure the organization's internal control continue to align with changing objectives, operating environment, laws and regulation, resources, and risks.

Common Terminology	Description
Ongoing Monitoring	• Regular Comparisons and Reconciliations • Automated Tools
Separate Evaluations	• Internal/External Audits • Self-assessments • Internal Control Testing
Baseline	The criteria and condition of the organization's internal control system at a specific point in time. Management can compare the baseline against the design of the future state of the internal control system because baseline consists of issues and deficiencies identified.
Control Deficiency	A potential or actual internal control issue or an opportunity to strengthen the organization's internal control system based on observation and/or direct testing.
Reportable Condition	A significant internal control deficiency that would adversely affect the organization's objectives and should be elevated to key personnel and senior management's attention. Management should develop proper guidelines for reporting these deficiencies.
Corrective Action	Action item planned by management to remediate identified internal control deficiencies in a specific time frame.