Overview:

To achieve an organization's goals, management should clearly define objectives to enable the identification of risks and define risk tolerances. Defining objectives not only allows management to identify risks but enhances the ability to analyze and respond to those risks. Objectives must exist before management can identify potential events which could affect their achievement.

The second component of the framework is Risk Assessment.

Risk Assessment provides the basis for developing appropriate risk responses. Management assesses the risks the entity faces from both external and internal sources.

Risk Assessment has four principles, and to help management and the oversight body to achieve each principle, there are attributes to each of the four principles.

Principle 6- Define Objectives and Risk Tolerances:

"Management should define objectives clearly to enable the identification of risks and define risk tolerances."

Attributes:

- Definition of objectives
- Definition of risk tolerances

Definition of Objectives:

Management defines objectives in specific and measureable terms to enable the design of internal control for related risks. Specific terms are fully and clearly set forth so they can be easily understood. This involves clearly defining what is to be achieved, who is to achieve it, how it is to be achieved, and the time frames for achievement. Measureable objectives are generally free of bias and do not require subjective judgements to dominate their measurement in quantitative or qualitative form. Management considers external requirements and internal expectations when defining objectives to enable the design of internal control.

Categories of Objectives:

Operational: Level of variation in performance in relation to risk.
Nonfinancial reporting: Level of precision and accuracy suitable for user needs, involving both qualitative and quantitative considerations to meet the needs of the nonfinancial report user.
Financial reporting: Judgements about materiality are made in light of surrounding circumstances, involve both qualitative and quantitative considerations, and are affected by the needs of financial report users and size or nature of a misstatement.
Compliance: Concept of risk tolerance does not apply. An entity is either compliant or not compliant.

Definition of Risk Tolerances:

Management defines risk tolerances for the defined objectives. Risk tolerance is the acceptable level of variation in performance relative to the achievement of objectives. Risk tolerance is often measured in the same terms as the performance measures for the defined objectives. When defining objectives, management considers risk tolerance in the context of the entity's applicable laws, regulations, and standards as well as the entity's standards of conduct, oversight structure, organizational structure, and expectations of competence. Management also evaluates whether risk tolerances enable the appropriate design of internal control by considering whether they are consistent with requirements and expectations for the defined objectives.

Principle 7- Identify, Analyze, and Respond to Risks:

"Management should identify, analyze, and respond to risks related to achieving the defined objectives."

Attributes:

- Identification of risks
- Analysis of risks
- Response to risks

Identification of Risks:

Identification of risk is necessary to provide a basis for analysis of risk. To properly identify risks, management must consider an organization's inherent and residual risk. Lack of response to risk can cause disruption in the internal control system. Management considers all significant interactions within the entity and with external parties, changes within the entity's internal and external environment, and other internal and external factors to identify risks throughout the entity.

Inherent risk: is the risk to an entity in the absence of management's response to the risk.
Control: the internal control implemented to mitigate the inherent risk.
Residual risk: is the risk that remains after management's response to inherent risk.
Risk equation: Inherent risk – Control = Residual risk

It is important to identify both internal and external events affecting achievement of an entity's objectives.

Internal Events	External Events
Implementation of new technology	New laws or regulations
Personnel changes	Updated standards
	Economic deficit

Analysis of Risks:

Management analyzes the identified risks to estimate their significance, which provides a basis for responding to the risks. Management estimates the significance of a risk by considering the magnitude of impact, likelihood of occurrence, and nature of the risk. Risks may be analyzed on an individual basis or grouped into categories with related risks and analyzed collectively.

Response to Risks:

Management designs responses to the analyzed risks so that risks are mitigated within the defined risk tolerances for the defined objectives. Based on the selected risk response, management designs the specific actions to respond to the analyzed risks. The nature and extent of the risk response actions depend on the defined risk tolerance.

Categories of Risk Response:

- **Acceptance:** No action is taken to respond to the risk based on the insignificance of the risk.
- **Avoidance:** Action is taken to stop the operational process or part of the operational process causing the risk.
- **Reduction:** Action is taken to reduce the likelihood and/or magnitude of the risk.
- **Sharing:** Action is taken to transfer or share risks across the entity or with external partners, such as insuring against losses.

Principle 8- Assess Fraud Risk:

"Management should consider the potential for fraud when identifying, analyzing, and responding to risks."

Attributes:

- Types of fraud
- Fraud risk factors
- Response to fraud risk

Types of Fraud:

- **Fraudulent financial reporting:** Intentional issuance of misleading financial statements in an effort to avoid negative opinions about the business/organization. This includes intentional misapplication of accounting principles; intentional omissions of transactions or disclosures in financial statements; intentional misrepresentation of estimates, such as revenue, receivables, or write-offs; manipulation of complex transactions or calculations; manipulation of financial or other data motivated by performance or other incentives.

- **Misappropriation of assets-** Theft of an entity's assets through theft of property, embezzlement of receipts, or fraudulent payments. Related fraud risks include inadequate supervisory controls over transactions; unchecked delegated authority; lack of budgetary controls at the appropriate level of operations; inadequate physical access controls; inappropriate access or inadequate data systems controls.

- **Corruption-** Bribery, collusion, management override of controls, and other illegal acts. Related fraud risks include the lack of audit committee or governing body oversight of operations; the lack of, or inadequate, oversight of a whistleblower reporting process; performance or other incentives that may motivate manipulation of financial or other data; unreasonable pressure to meet goals; failure to uphold a culture of accountability, ethical conduct, and integrity; disregard of statutory, regulatory, or other compliance requirements; inadequate segregation of duties; inappropriate access or inadequate data systems controls.

Fraud Risk Factors:

It is essential to consider fraud, waste, and abuse in your risk assessment. Not only is it important to assess the risk of fraudulent financial reporting or misappropriation and corruption but also abuse or misuse of authority or position for personal benefit. Waste and abuse may not involve illegal acts, yet are still a risk to consider and may be an indication of fraud. Fraud risk factors include pressure, opportunity, and rationalization.

Pressure- motivation such as debt problems or pressure from upper management to reach goals.
Opportunity- ability to abuse or exploit position with low risk of being discovered.
Rationalization- justification for fraudulent action, such as the need to take care of family or lack of oversight.

Fraud risk may be the highest when all three factors are present, but the presence of one or more factors may indicate a fraud risk. In addition, management should consider other information from available internal and external sources. Information may include allegations of fraud reported to internal audit, human resources, the Comptroller of the Treasury, grantors, federal agencies or other affiliated entities.

Fraudulent events differ from errors as they are always intentional.

Examples of Fraudulent Events:

Fraudulent financial reporting	Corruption	Misappropriation of assets
Alteration of records	Bribery/Kickbacks	Theft of assets
Not adhering to accounting principles	Management override of controls	Fraudulent payments to vendors
Omissions of amounts	Blackmail	

Questions to consider in assessing the potential for fraud:

- What pressures exist to reduce spending, improve timeliness of services, increase clients served, or reduce staff?
- What salary incentives exist for leadership?
- What mitigating controls, oversight, or organizational changes will reduce the opportunity for fraud in at-risk areas?
- Is there sufficient integrity in the data used to manage operations? How is integrity assured?
- Is the internal audit function adequately staffed and provided direct access to the audit committee or the governing body without restriction?

Principle 9- Identify, Analyze, and Respond to Change:

"Management should identify, analyze, and respond to significant changes that could impact the internal control system."

Attributes:

- Identification of change
- Analysis of and response to change

Identification of Change:

As a part of risk assessment or a similar process, management identifies changes that could significantly impact the entity's internal control system. Identifying, analyzing, and responding to change is and should be considered part of the entity's regular risk assessment process. Conditions affecting the entity and its environment continually change. Management can anticipate and plan for significant changes by using a forward-looking process for identifying change.

Analysis of and Response to Change:

Management maintains an effective internal control system by analyzing and responding to changes and the related risks within the entity and the environment in which it operates. Changes in conditions affecting the entity often require changes to the internal control system since existing controls may no longer be effective for meeting objectives or addressing risks. For example, management should consider changes that occur in leadership, the business model, or its external environment by revising the internal control system on a timely basis to maintain its effectiveness. Significant changes to the entity should prompt management to perform a revised risk assessment to identify, analyze, and respond to any new risks and may require additional assessment to determine whether previously defined risk tolerances and risk responses need to be revised.

Questions to consider in identifying and assessing changes impacting internal control:

- What funding changes occurred in the last year?
- What statutory changes occurred in the last year?
- Has key leadership changed in the last year?
- Are there any new programs planned or are any programs closing out?
- What are the key changes in accounting standards since the prior year?