ENTITY-WIDE RISK ASSESSMENT

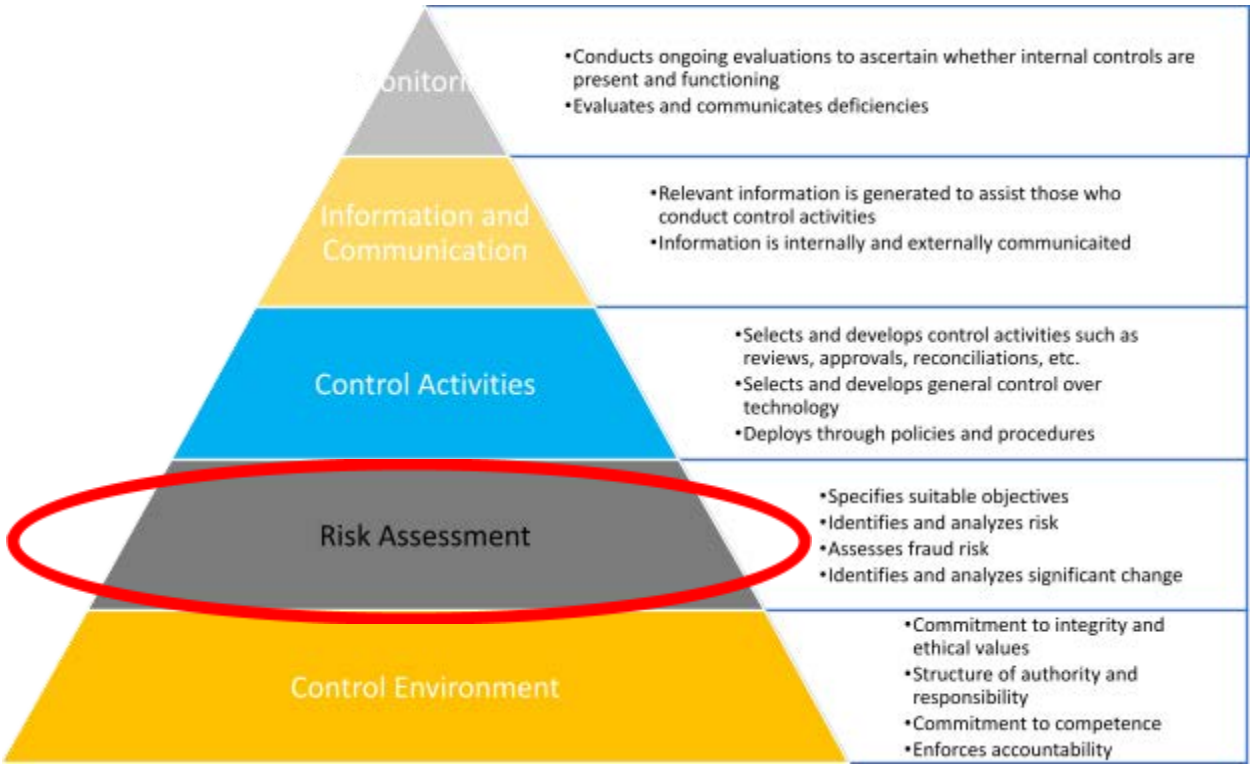
Introduction

All executive branch agencies must conduct an annual risk assessment using a methodology which applies leading practices. Agencies should share two or three high or critical risks and their plans to address them.

Effective risk assessment enables organizations to better anticipate challenges so they can get ahead of them. Obtaining robust information on risk allows management, in the face of finite resources, to assess overall resource needs, prioritize resource deployment and enhance resource allocation. A risk assessment without shared definitions and an understanding of the product it will produce will likely be viewed as not successful; therefore, the definitions below help establish shared definitions and understanding.

Definitions

COSO's Internal Control Framework – A generally accepted internal control framework that defines how to respond to and manage risk and that is designed to help organizations enhance the likelihood of achieving their objectives. Risk assessment is one component of this framework as illustrated below.



Internal Audit – The individuals who operate independent from management to provide assurance and insight on the adequacy and effectiveness of governance and on the management of risk, including internal controls.

Internal Control – The processes, actions and activities designed to create reasonable assurance of the achievement of objectives.

Management – The individuals, teams and support functions assigned to provide products and/or services to the organization's clients.

Risk – Anything that threatens an organization's ability to achieve its goals.

Risk Assessment – One of the five components of the COSO Internal Control Framework. It addresses how an organization identifies, assesses and manages risks related to the achievement of objectives. Typically results in a report on risk by priority.

Risk and Control Types – Risks and controls are often grouped into types (such as strategic, operational or hazard) to facilitate risk identification and control development.

Risk Rating – A scale by which a risk is compared to how likely/probable it is to occur and what impact it would have on the achievement of objectives when it occurs.

Risk Types – A classification label used to identify and characterize the variety of risk to which an organization is exposed. Typical risk types include:

- Strategic Risk – Risks that arise when an organization's strategy fails to deliver expected outcomes. These are the risks taken when making strategic decisions. They are typically mitigated through formal decision-making processes that vet the data involved in choices and that check for decision bias. They also include organizational impacts by diverting resources to a strategic choice. Examples include:
    - Ethics, conflicts of interest, bias in decision-making processes.
    - Strategic decisions that are unclear or poorly communicated.
    - The introduction of new programs or services.
    - Changes in senior management.
    - Changes to customer demands or expectations.
    - Financial challenges (e.g., underfunded programs).
    - Problems with suppliers, vendors or other stakeholders.
- Operational Risk – Risks that arise from inadequate or failed internal procedures, employee errors, cybersecurity events or external events. These are the risks that arise due to an absence of or weakness in operational controls. As management sets up operations, there is an expectation that people with needed skills are involved, processes are efficient and effective, and technology is enabling and supportive. There is also an expectation that management has oversight mechanisms needed to enable operational success and capacity growth over time. Examples include:
    - Weakness in governance and management oversight controls.
    - Unclear objectives and accountabilities.
    - Misalignment of people, processes and technology.
    - Inadequate or failed internal processes.

    - Human error.
    - System downtime or failure.
    - Inadequately trained staff.
    - Breakdown of process controls.
- Hazard Risk – The many things that could go wrong, mostly external to the organization. Management typically controls these risks by funding functions to address them (e.g., insurance, communications, information security, legal, safety, etc.) Examples include:
    - Damage to the organization's credibility or reputation.
    - Compliance with laws, rules or policies.
    - Information security.
    - Human resource incidents (e.g., workplace harassment and employee discipline).
    - Cybersecurity events (e.g., data breaches).
    - Fraud.
    - External events (e.g., earthquakes or pandemics).

Conducting an Entity-Wide Risk Assessment

1. Who is Responsible?
   Management is responsible for managing risks to the entity; therefore, ensuring a risk assessment is conducted is ultimately their responsibly. Internal audit standards and leading practices put internal audit in a position to lead or participate in conducting the entity-wide risk assessment.

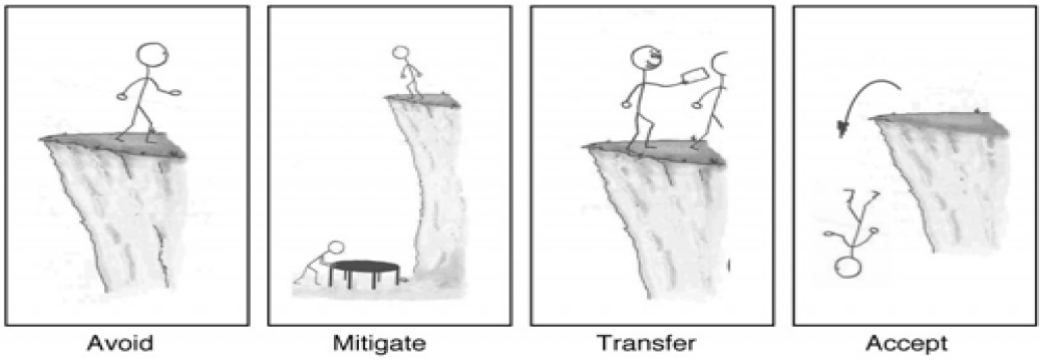
   Defining risks requires an analytical mind that can take off the operational hat and put on a value-preservation hat. It is possible that several individuals may be needed to form a risk assessment leadership committee to execute it with competence.

2. Develop a Risk Assessment Strategy
   The following should be considered when developing a risk assessment strategy:

    - Timing – Choose a period of time when key individuals can give sufficient attention and thought to the assessment (e.g., not during a legislative session).
    - Frequency – Risk assessments should be conducted at least annually.
    - Methodology:
        - Background – Gain an understanding of what is at risk, including the operational structures, strategic plans and objectives of the organization.
        - Scope – This is critical to the risk assessment being viewed as successful. Scoping entails the following:
            - Knowing which risk types will be covered and how they will be prioritized, given the time and resources available.
            - Defining if the risk assessment will be wide covering all areas of the organization or deep in only a few areas of the organization.
        - Research – Based on the scope of the risk assessment, define and collect risks through research, interviews, surveys or workgroups with identified personnel.
        - Risk Type – Defining potential risks by risk types in advance is helpful to all involved as it aids in communication and in the development of risk assessment methodology. This can help management view risk through the internal controls

they have naturally put in place as they seek the success of strategic and operational objectives.

- Rating - Rate the impact and likelihood/probability of identified risks.
- Risk Response - Develop a risk response that may include one of the following:



  - Avoid – Eliminate the risk by choosing not to participate in programs or activities considered too risky.
  - Mitigate – Reduce the impact and likelihood/probability of the risky event by applying internal controls.
  - Transfer – Contract with a third party to administer the program or activity, thus transferring the risk and loss exposure.
  - Accept – Retain the risk and develop plans to cover the financial or non-financial consequences.

- Communicate the results to appropriate parties in a written format.

3. <u>Utilizing Risk Assessments</u>
   Management should utilize risk assessments to develop risk management strategies and the annual audit plan.