Key ERM Terms

Context: The area or circumstances around which risk management activities occur. The context for a risk assessment, for example, could be the entire organization, an organizational component, or an initiative.

Enterprise risk management (ERM): The capabilities and practices used to identify, assess, and respond to risk, the uncertainties (threats and opportunities) that may impact goals and objectives. ERM results in a top-down, holistic view of the organization's most significant threats and opportunities.

Environment, external: External environment in which the organization seeks to achieve its objectives, including cultural, social, political, legal, regulatory, financial, technological, economic, natural, and competitive environments, whether international, national, regional, or local; key drivers and trends; and relationships with, perceptions, and values of external stakeholders.

Environment, internal: Internal environment in which the organization seeks to achieve its objectives, which can include governance, organizational structure, policies, resource and knowledge capabilities, information systems and flows, decision-making processes, culture, form and extent of contractual relationships, and relationships with, perceptions, and values of internal stakeholders.

Event: Occurrence or change of a particular set of circumstances. Can be one or more occurrences, can have several causes, and can consist of something not happening.

Impact (consequence): The extent to which an event might positively or negatively affect the organization. Impact may fall into any of the following categories: financial, reputational, regulatory, health, safety, security, environmental, employee, stakeholder, or operational.

Likelihood: The chance that something will happen, expressed quantitatively, using the best judgement of responsible officials.

Responsible official (RO): Office or official with the accountability and authority to respond to a risk.

Risk: A potential event (an uncertainty)—either positive (opportunity) or negative (threat)—that may impact an organization's ability to achieve its goals and objectives.

Risk assessment: Overall process of identifying, analyzing, and evaluating risks (uncertainties) with the goals of assisting in strategy-setting, decision-making, and resource allocation; assuring stakeholders that risks are appropriately addressed; and improving outcomes in achieving goals and objectives.

Risk response: Process to respond to a risk, involving one or a combination of the following:

For negative risks (threats):

Avoid: An informed decision not to be involved in, or to withdraw from, an activity, in order not to be exposed to a particular risk.

Accept: An informed decision to tolerate a particular risk and take no additional action.

Mitigate/Reduce: Take actions designed to reduce a risk or its consequences. Usually requires an action plan to address.

Share/Transfer: Transfer risk, preferably contractually, to other parties, including insurance.

For positive risks (opportunities):

Ignore: An informed decision, based on currently available information, to decline to pursue a potential opportunity or consider it further.

Share: Partner, subcontract with, or acquire another party to pursue the opportunity or refer the opportunity to another party.

Defer: Postpone immediate action to monitor evolving circumstances surrounding the opportunity and/or to gain additional knowledge.

Pursue: An informed decision, based on currently available information, to create an action plan to be involved in an activity or event that would increase the chances of achieving goals and objectives

Risk response plan: Plan to implement chosen risk response. Action plans should include the following: tasks, position/persons assigned to tasks, timeframe for completion, and resource requirements. Response plans may be focused on mitigation of threats or pursuit of opportunities.

Risk statement: Structured statement of risk that describes the potential event and its impact on the achievement of goals and objectives. Whenever possible, the statement should also contain the cause or trigger for the event.