Key ERM Terms and Definitions

General ERM Terms

Enterprise risk management (ERM): A structured, consistent, and continuous process across the whole organization for identifying, assessing, deciding on responses to, and reporting on opportunities and threats that affect the achievement of its objectives. (IIA)

ERM framework: Set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing, and continually improving risk management throughout the organization at all levels. Ensures that info about risk derived from the risk management process is adequately reported and used as basis for decision-making and accountability at all relevant organizational levels.

Risk: Any issue (positive or negative) that may impact an organization's ability to achieve its objectives; the effect of uncertainty on organizational objectives. Often characterized in reference to potential events, consequences, and the likelihood thereof.

Terms Related to ERM Program & Context

Context, 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.

Context, 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.
values, behaviors and understanding of risk in the entity.

ERM goals (objectives): Goals and objectives that ERM activities are seeking to achieve; what the ERM program and process should accomplish for an organization

ERM guiding principles (cultural expectations): Description of the risk-aware culture or control environment; expectations regarding behaviors, communication, information-sharing, reporting, etc.

ERM policy: Statement of the overall intentions and direction of the entity in regard to ERM. Describes principles, requirements, and restrictions, and establishes standards, rights and responsibilities that guide individuals in their pursuit of entity goals

Governance: The entity's tone and reinforcement and establishment of oversight responsibilities and processes for enterprise risk management. Governance differs from culture in that culture represents the ethical values, behaviors and understanding of risk in the entity.

Responsible official (risk owner): Person or entity with the accountability and authority to manage a risk

Risk Appetite: The amount and type of risk that an organization is willing to accept in order to meet its strategic objectives. Organizations will have different risk appetites depending on their sector, culture and objectives. A range of appetites exist for different risks and these may change over time

Risk philosophy: Statement of the overall intentions, direction, and attitude of the entity related to risk; reflected in the ways risks are considered in both strategy development and day-to-day operations. The organization's approach to assess and eventually pursue, retain, take, or turn away from risk.

Terms Related to the Risk Assessment Process

Acceptance: Form of risk response, an informed decision to tolerate or take on a particular risk

Avoidance: Form of risk response, an informed decision not to be involved in, or to withdraw from, an activity, in order not to be exposed to a particular risk.

Control activity: A process, effected by an entity's board of directors (can substitute oversight body here), management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.

Enhance: The opportunity equivalent of "mitigating" a risk is to enhance the opportunity. Mitigation modifies the degree of exposure by reducing probability and/or impact, whereas enhancing seeks to increase the probability and/or the impact of the opportunity in order to maximize the benefit to the project.

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.

Exploit: Parallels the "avoid" response, where the general approach is to eliminate uncertainty. For opportunities, the "exploit" strategy seeks to make the opportunity definitely happen (i.e. increase probability to 100%). Aggressive measures are taken which seek to ensure that the benefits from this opportunity are realized by the project.

Ignore: Just as the "acceptance" strategy takes no active measures to deal with a residual risk, opportunities can be ignored, adopting a reactive approach without taking explicit actions.

Impact (consequences): Outcome of an event affecting objectives, either positively or negatively. Can be certain or uncertain; can be expressed qualitatively or quantitatively. An event can lead to a range of consequences, and initial consequences can escalate through knock-on effects.

Likelihood: The chance that something will happen – whether defined, measured, or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically

Opportunity response (treatment): Process to modify or respond to an opportunity. Opportunity response can involve one or a combination of: exploitation, ignoring, enhancement, or sharing.

Probability: Measure of the chance of occurrence expressed as a number between 0 and 1

Reduce: Form of risk response involving actions designed to reduce a risk or its consequences.

Risk analysis: Process to comprehend the nature of risk and to determine the level of a risk; provides the basis for risk evaluation and decisions about risk response.

Risk assessment: Overall process of identifying, analyzing, and evaluating risk

Risk criteria: Terms of reference against which the significance of a risk is evaluated.

Risk evaluation: Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude are acceptable or tolerable. Use of a tool/system to rate and/or prioritize a series of risks.

Risk financing: Form of risk response, involving contingent arrangements for the provision of funds to meet or modify the financial consequences should they occur

Risk identification: Process of finding, recognizing, and describing risks

Risk inventory, preliminary: Preliminary list of potential risks identified for further assessment and analysis.

Risk portfolio (profile): A composite view of highest-level entity risk exposures for presentation by management and discussion with the Board; provides information regarding relationships, concentrations, and/or overlaps of risk as they relate to strategic objectives. Description of any set of risks.

Risk register (log, repository): Record of information about identified risks; the complete list of all risks identified in the ERM process

Risk response (treatment): Process to modify or respond to a risk. Risk response can involve one or a combination of: avoidance, acceptance, reduction, or transfer.

Risk response plan: Plan to implement chosen risk response.

Risk statement (description): Structured statement of risk usually containing four elements: sources, events, causes, and impacts/consequences.

Sharing (transfer), opportunity: The “transfer” response allocates ownership to a third party best able to deal with the threat. Similarly, a “share” strategy for opportunities seeks a partner able to manage

the opportunity, who can maximize the chance of it happening and/or increase the potential benefits. This will involve sharing any upside in the same way as risk transfer involves passing penalties.

Sharing (transfer), risk: Form of risk response, involving contractual risk transfer to other parties, including insurance.

Source (of risk): Element or circumstance which alone or in combination has the intrinsic potential to give risk to risk. Can be tangible or intangible.

Terms Related to ERM-Enabling Activities

Communication & consultation: Continual and iterative processes that an organization conducts to provide, share, or obtain information, and to engage in dialogue with stakeholders regarding the management of risk

Monitoring: Continual checking, supervising, critically observing, or determining the status in order to identify change from the performance level required or expected. Can be applied to an ERM framework, ERM process, risk, or control.

Reporting: Form of communication intended to inform particular internal and external stakeholders by providing information regarding the current state of risk and its management.