Acceptable risk

the part of identified risk that is allowed to persist after controls are applied. Risk can be determined acceptable when there is slack of money or when further efforts to reduce it would cause degradation of the probability of success of the operation, or when a point of diminishing returns has been reached.

Communication and consultation

continual and iterative processes that an organization conducts to provide, share or obtain information and to engage in dialogue with stakeholders and others regarding the management of risk. The information can relate to the existence, nature, form, likelihood, severity, evaluation, acceptability, treatment or other aspects of the management of risk. Consultation is a two-way process of informed communication between an organization and its stakeholders or others on an issue prior to making a decision or determining a direction on a particular issue. Consultation is:

- a process which impacts on a decision through influence rather than power; and
- an input to decision making, not joint decision making

Control

any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. These actions may be taken to manage either the impact if the risk is realised, or the frequency of the realization of the risk. Controls include any plan, process, policy, device, practice, or other actions which modify risk, and organize and direct the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved. Controls may not always exert the intended or assumed modifying effect. Risk treatments become controls, or modify existing controls, once they have been implemented.

Enterprise-wide 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.

Establishing the context

defining the external and internal parameters to be taken into account when managing risk, and setting the scope and risk criteria for the risk management policy.

Event

occurrence or change of a particular set of circumstances. An event can be one or more occurrences, and can have several causes. An event can consist of something not happening. An event can sometimes be referred to as an “incident” or “accident”.

External context

external environment in which the organization seeks to achieve its objectives. External context can include:

- the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;
- key drivers and trends having impact on the objectives of the organization; and
- relationships with, and perceptions and values of, external stakeholders.

Identified risk

that risk that has been determined to exist using analytical tools. The time and costs of analysis efforts, the quality of the risk management program, and the state of the technology involved affect the amount of risk that can be identified.

Inherent risk

the risk to an entity in the absence of any actions management might take to alter the risk’s likelihood or impact. These risks may result from an entity’s industry, strategy, and environmental factors.

Internal context

internal environment in which the organization seeks to achieve its objectives. Internal context can include:

- governance, organizational structure, roles and accountabilities;
- policies, objectives, and the strategies that are in place to achieve them;
• the capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);
• perceptions and values of internal stakeholders;
• information systems, information flows and decision-making processes (both formal and informal);
• relationships with, and perceptions and values of, internal stakeholders;
• the organization's culture, the integrity, ethical values;
• standards, guidelines and models adopted by the organization;
• form and extent of contractual relationships.

Impact
represents the potential effects and consequences that a given event could have on an entity and its objectives. An event can lead to a range of consequences. A consequence can be certain or uncertain and can have positive or negative effects on objectives. Events that have positive effects represent opportunities and those with negative effects represent risks. Consequences can be expressed qualitatively or quantitatively. Entities often describe events based on severity, effects, or monetary amounts. Initial consequences can escalate through knock-on effects.

Level of risk
magnitude of a risk, expressed in terms of the combination of consequences and their likelihood.

Likelihood
the possibility that an event may occur. It can be defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and it can be described using qualitative terms (such as high, medium, and low) or quantitative measures (such as a percentage and frequency).

Monitoring
continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected. Monitoring can be applied to a risk management framework, risk management process, risk or control.

Residual risk
the portion of total risk remaining after risk treatment has been applied. Residual risk comprises acceptable risk and unidentified risk. Management must decide whether this residual risk is within the entity's risk appetite. Residual risk is also known as "retained risk".

Risk
the possibility of an event occurring that will have an effect on the achievement of objectives. An effect is a deviation from the expected (positive and/or negative). Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process). All activities of an organization involve risk. Organizations manage risk by identifying it, analysing it and then evaluating whether the risk should be modified by risk treatment in order to satisfy their risk criteria. Risk is often characterized by reference to potential events and impact, or a combination of these. Risk is measured in terms of impact (including changes in circumstances) and likelihood of occurrence. Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of an event, its consequences, or likelihood.

Risk analysis
process to comprehend the nature of risk and to determine the level of risk. Risk analysis provides the basis for risk evaluation and decisions about risk treatment. Risk analysis includes risk estimation.

Risk attitude
organization's approach to assess and eventually pursue, retain, take or turn away from risk.

Risk aversion
attitude to turn away from risk.

Risk criteria
terms of reference against which the significance of a risk is evaluated. Risk criteria are based on organizational objectives, and external and internal context. Risk criteria can be derived from standards, laws, policies and other requirements.

**Risk exposure**

the consequences, as a combination of impact and likelihood, which may be experienced by an organization if a specific risk is realized.

**Risk identification**

process of finding, recognizing and describing risks. Risk identification involves the identification of risk sources, events, their causes and their potential consequences. Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and stakeholder’s needs.

**Risk management**

coordinated activities to direct and control an organization with regards to risk.

**Risk management framework**

the totality of the structures, methodology, procedures and definitions that an organization has chosen for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization. The foundations include the policy, objectives, mandate and commitment to manage risk. The organizational arrangements include plans, relationships, accountabilities, resources, processes and activities. The risk management framework is embedded within the organization's overall strategic and operational policies and practices.

**Risk management plan**

scheme within the risk management framework specifying the approach, the management components and resources to be applied to the management of risk. Management components typically include procedures, practices, assignment of responsibilities, sequence and timing of activities. The risk management plan can be applied to a particular product, process and project, and part or whole of the organization.

**Risk management policy**

statement of the overall intentions and direction of an organization related to risk management.

**Risk management process**

systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring and reviewing risk in order to provide reasonable assurance regarding the achievement of the organization’s objectives.

**Risk map**

a graphic representation of likelihood and impact of one or more risks. Risk maps may plot quantitative or qualitative estimates of risk likelihood and impact. Often, risk maps are referred to as "heat maps" since they present risk levels by color, where red represents high risk, yellow moderate risk, and green low risk.

**Risk maturity**

measuring the level of development of risk management practices within an organization, based on different variables and / or dimensions characterized by organizational behaviors and indicators.

**Risk measurement**

assigning values to each risk using the defined criteria. Most organizations define scales for rating risks in terms of impact, likelihood, and other dimensions.

**Risk owner**

person or entity with the accountability and authority to manage the risk.

**Risk profile**

description of any set of risks. The set of risks can contain those that relate to the whole organization, part of the organization, or as otherwise defined.

**Risk register/risk log**

a master document that records identified risks, their severity, and the responses to be taken.
Risk source

element which alone or in combination has the intrinsic potential to give rise to risk. A risk source can be tangible or intangible.

Risk Strategy

the overall organizational approach to risk management as defined by the entity governing risk management. This should be documented and easily available throughout the organization.

Risk tolerance

the acceptable level of variation relative to achievement of a specific objective. This variation is often measured using the same units as its related objective. In setting risk tolerance, management considers the relative importance of the related objective and aligns risk tolerances with risk appetite. Therefore, an entity operating with its risk tolerances, narrow boundaries, is operating within its risk appetite, wide boundaries.

Risk treatment

means by which an organization elects to manage individual risks. Risk treatments can also be called risk responses. As part of enterprise risk management, for each significant risk an entity considers potential responses from a range of response categories. Risk treatment can involve:

- **Avoidance/Terminating** is a response where you exit the activities that cause the risk. Some examples of avoidance are exiting product line, selling a division, or deciding against expansion.
- **Treating/Reduction** is a response where action is taken to mitigate the risk likelihood and impact, or both.
- **Transferring/Sharing** is a response that reduces the risk likelihood and impact by sharing or transferring a portion of the risk. An extremely common sharing response is insurance.
- **Tolerance/Acceptance** is a response where no action is taken to affect the risk likelihood or impact.
- Risk treatments that deal with negative consequences are sometimes referred to as "risk mitigation", "risk elimination", "risk prevention" and "risk reduction". Risk treatment can create new risks or modify existing risks.

Risk weighting

process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable. It’s the process of determining risk management priorities by comparing the level of risk against predetermined target risk levels and tolerance thresholds. Risk evaluation assists in the decision about risk treatment.

Review

activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives. Review can be applied to a risk management framework, risk management process, risk or control.

Stakeholder

person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity. A decision maker can be a stakeholder.

Total risk

the sum of identified and unidentified risk. Ideally, identified risk will comprise the larger proportion of the two.

Unacceptable risk

the portion of identified risk that cannot be tolerated, but must be either eliminated or controlled.

Unidentified risk

that risk that has not yet been identified. Some risk is not identifiable or measurable. Mishap investigations may reveal some previously unidentified risks.