



GLOSSARY

Glossary

accept

A risk response that means the organization takes the chance that the risk will occur, with full impact on objectives if it does.

avoid

A risk response that seeks to eliminate a threat by making the situation certain.

backlog

A list of new features for a product. The list may be made up of user stories which are structured in a way that describes who wants the feature and why. It is also a generic term that can be defined in terms of releases, sprints, and products.

benefit

The measurable improvement resulting from an outcome perceived as an advantage by the investing organization(s) and which contributes towards one or more organizational objectives.

competence

The ability to do something successfully.

contingency

A provision for a potential future situation.

contingent plan

A reactive risk response designed to be used if existing controls and any other proactive risk responses are unsuccessful.

continual improvement

A delivery mode used for improvement work that enables an organization to identify waste or redundancy in a product, service, process, or system. Work to eliminate this creates releases of additional value.

corporate governance

The means by which an organization is directed and controlled. At the level of the legal entity, corporate governance is focused on maintaining a sound system of internal control by which the directors and officers of the organization ensure that effective management systems are in place to protect assets, earning capacity, and the reputation of the organization.

correlation

The statistical dependence between two or more variables; for example, activities in a schedule that rely on the same resource for their completion.

current/net assessment

The largest realistic likelihood of occurrence or size of impact of a risk, assuming that all existing controls are implemented and effective. Also known as residual risk.

decision bias

The inherent tendency for people to adopt mental short cuts (heuristics) or faulty thinking processes (cognitive biases) to process situations and make decisions.

decision gate

An approval point where members of a governing body are required to decide how to proceed. Alternatively referred to as stage gates or stage boundaries.

delegated limits of authority

Clarification of the responsibilities of decision-makers relating to defined objectives, including commitment of expenditure and legal undertakings.

deterministic

A situation or plan where the outputs are predicted assuming a fixed order and fixed parameters.

downside risk

A negative threat to objectives that would destroy planned value if it occurred.

enhance

A risk response for an opportunity that seeks to increase the likelihood and/or impact.

enterprise agility

A condition of an organization that is able to be flexible and responsive to drivers in its environment. Enterprise agility (also called 'corporate agility' or 'organizational agility') enables the organization to remain resilient.

enterprise risk management (ERM)

The culture, capabilities, and practices that are effected by an organization's management and applied in strategy-setting and across the entire enterprise or legal entity. ERM identifies and manages risk to be within an organization's risk appetite, and provides reasonable assurance regarding the achievement of organizational objectives.

expected value

The product of the estimated most likely impact of a risk and the estimated likelihood expressed as a percentage. Where the impact is financial, it is known as the expected monetary value.

exploit

A risk response for an opportunity that seeks to make the situation certain.

financial contingency

The financial allowance that decision-makers provide to deal with identified and unidentified risks.

functional orientation

An operating model primarily organized as a hierarchy, with specialists deployed in each function; for example, marketing, sales, manufacturing, logistics, procurement, accounts, compliance, human resources, customer services, etc.

futures thinking

A mindset and process focused on divergence, with a focus on possibilities. The opposite is analytical thinking, which seeks to create convergence and provide definite answers.

hybrid project delivery mode

A project delivery mode that combines a linear/sequential delivery mode for some phases or activities with an iterative/agile delivery mode for others.

impact

The estimated effect on objectives should a risk occur.

inherent/gross assessment

The largest realistic likelihood of occurrence or size of impact of the risk, assuming either that no controls exist, or that all controls or other actions fail.

issue

An unplanned event that has occurred and requires management action. An issue may be a problem, a query, a change request, or a risk that has occurred.

iterative/agile project delivery mode

A project delivery mode that repeats aspects of the design or delivery with the objective of managing any uncertainty of scope by allowing outputs to evolve as learning and discovery take place.

leading indicator

An observable and/or measurable instance that is evidence of the likelihood and/or size of impact of a risk beginning to change. It is the opposite of a lagging indicator which is only observable after the change. Alternatively called an early warning indicator.

likelihood

The estimated chance that a risk will occur. Likelihood is often estimated by considering probability or frequency.

linear/sequential project delivery mode

A project delivery mode that aims to complete the delivery of outputs within a single pass through a set of distinct phases, completed in sequence.

multimodal delivery

The selection of methods of delivering the work that are appropriate to the task, the team, the individuals (including customers, stakeholders, leaders, and workers), and the context.

neutral facilitator

A person who is independent of the risk analysis and management work being performed, and who has the skills to help the group come to an unbiased set of decisions about risks and their priority.

operation

The routine running and management of an activity, product, or service.

portfolio

The totality of an organization's investment (or segment thereof) in the changes required to achieve its strategic objective.

principal risk

A risk that, if it occurred, would have a material effect on the current performance, future prospects, and/or reputation of an organization.

principle

A guiding obligation that is continually required to create and protect value from risk management.

proactive risk response

An action that is taken in advance of a risk occurring to attempt to influence the likelihood of its occurrence and/or the size of its impact.

probabilistic

A situation or plan where the outputs are predicted, taking into account variability and randomness. Alternatively called stochastic.

process

A structured set of activities that define the sequence of actions and their inputs and outputs to achieve a specific objective.

process cycle

A continuous sequence of processes, starting with the 'define context and objectives' process, and repeated as necessary to ensure that the organization has an up-to-date view of the risks it faces in order to support effective decision-making.

product

An output of a design and development process that is delivered to create value for the organization and/or end-user. Products can be physical assets or services.

product orientation

An operating model primarily organized around self-managed teams focused on the development, launch, support, renewal, and replacement or retirement of products and services.

programme

A temporary structure designed to lead multiple interrelated projects and other work in order to progressively achieve outcomes of benefit for one or more organizations.

project

A temporary organization that is created for the purpose of delivering one or more business products according to an agreed business case.

proxy measure

A measurable variable that is an indirect but strongly correlated measure of the desired outcome. An example would be measuring the number of customer complaints as a proxy measure for determining customer satisfaction.

qualitative

Related to the quality of a variable rather than the quantity.

quantitative

Related to the quantity of a variable rather than the quality.

reactive risk response

An action that is planned to be implemented if a risk occurs to control the size of impact.

reduce

A risk response to a threat that seeks to reduce likelihood and/or impact.

resilience

The ability of a person or an organization to deal with unplanned events and respond strongly, ideally addressing not only anything that has been lost, but turning the adversity into an opportunity for greater value to be created in future.

risk

An uncertain event or set of events that, should it occur, will have an effect on the achievement of objectives. Risk is a neutral concept; risks can either be threats (downside risks) or opportunities (upside risks).

risk action owner

The person who is the nominated owner of agreed actions to respond to a risk. Also known as the risk actionee.

risk appetite

The amount and type of risk that the organization is willing to take in pursuit of its objectives.

risk capacity

The amount and type of risk that the organization is able to take in pursuit of its objectives.

risk culture

The patterns of day-to-day, risk-based, decision-making behaviours shared by a group of people with a common purpose.

risk exposure

The degree to which a particular objective is 'at risk'. Risk exposure is a neutral concept; exposure can be positive or negative.

risk management

The coordinated direction and control of an organization undertaken to protect and create value in the face of risk.

risk owner

The person who is assigned to take responsibility for responding to a risk to the satisfaction of the relevant governance board.

risk perception

The way in which a stakeholder views a risk, based on a set of values or concerns.

risk proximity

How near in time a risk might occur.

risk tolerance

A measurable threshold to represent the tolerable range of outcomes for each objective 'at risk', using the same units as for measuring performance for that objective.

risk velocity

How quickly a risk would have an impact on objectives should it occur.

secondary risk

A risk that arises directly as a result of implementing a risk response.

share

A risk response where a third party takes responsibility for an aspect of the risk. Also known as 'transfer'.

stakeholder

Any individual, group, or organization that can affect, be affected by, or perceives itself to be affected by, organizational objectives.

stakeholder engagement

A way of exercising influence and achieving positive outcomes through effective management of relationships.

strategy

A broad approach or course of action defined by an organization for achieving its objectives.

target/future net assessment

The likelihood of occurrence of the risk and the size of impact on objectives, assuming that all existing controls and additional proactive responses are implemented and effective.

three-lines model

An approach that enables organizations to establish strong governance and risk management through three levels of assurance in line with delegated authority within the organization. Formerly known as the three lines of defence.

timebox

A finite period of time when work is carried out to achieve a goal or meet an objective.

triple bottom line

A sustainability-based accounting framework that focuses on environmental, social, and financial performance.

upside risk

A positive opportunity that would create additional value if it occurred.

value

The perceived benefits, usefulness, and/or importance of an outcome in proportion to the resources deployed to achieve it.

weak signal

Emerging, unusual information that may be an early indicator of significant disruption or change.