

RISK MANAGEMENT PROCESS



1. Risk assessment

1.1 Risk identification

The purpose of risk identification is to find, recognize and describe risks that might help or prevent an organization achieving its objectives, using one or more of the following dimensions:

- tangible and intangible sources of risk.
- causes and events.
- threats and opportunities.
- vulnerabilities and capabilities.
- changes in the external and internal context.
- indicators of emerging risks.
- the nature and value of assets and resources.
- consequences and their impact on objectives.
- limitations of knowledge and reliability of information.
- time-related factors.
- biases, assumptions, and beliefs of those involved.

Organization should identify risks, no matter their sources are under its control.

1.2 Risk analysis

The purpose of risk analysis is to comprehend the nature of risk and its characteristics including, where appropriate, the level of risk. Risk analysis involves a detailed consideration of uncertainties, risk sources, consequences, likelihood, events, scenarios, controls, and their effectiveness. For example, food manufacture entails quality risk. Bad processing may have catastrophic effect say 5 on a 5-point scale. However, processing procedures may be so good that chances of bad processing taking place could be 1 on a 5-point scale. This would then mean that the risk score is $5 \times 1 = 5$.

1.3 Risk evaluation

The purpose of risk evaluation is to support decisions. Risk evaluation involves comparing the results of the risk analysis with the established risk criteria to determine where additional action is required. This can lead to a decision to:

- do nothing further. (For example, the board may set the risk criterion at 6)
- consider risk treatment options. (in case the board sets the risk criterion at 3)
- undertake further analysis to better understand the risk; (reviewing the risk score of 5)
- maintain existing controls. (in case the board sets the risk criterion at 5)
- reconsider objectives. (outsource food manufacture, for example)

2. Risk treatment

2.1 Options for treating risk may involve one or more of the following:

- avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk. To continue with the same example, if quality risk can't be contained, stop processing food.
- taking or increasing the risk to pursue an opportunity. When providing security to a factory is too risky in a flood zone, management is motivated to relocate the factory to a safer zone which may be an opportunity.
- removing the risk source. Relocating the factory in the above example is removing a risk source.
- changing the likelihood. For example, when audit frequency is increased, chances of fraud and error are likely to reduce.
- changing the consequences. Effluence treatment is a good example to change a bad consequence.
- sharing the risk (eg. through contracts, buying insurance); and
- retaining the risk by informed decision. Because for example, other alternatives may be riskier.

Justification for risk treatment is broader than solely economic considerations and should consider the organization's obligations, voluntary commitments, and stakeholder views (like decommissioning, taking environmentally friendly actions, and other Environment, Social and Governance considerations).

2.2 Preparing and implementing risk treatment plans


The information provided in the treatment plan should include:

- the rationale for selection of the treatment options, including the expected benefits to be gained.
- those who are accountable and responsible for approving and implementing the plan.
- the proposed actions.
- the resources required, including contingencies.
- the performance measures.
- the constraints.
- the required reporting and monitoring.
- when actions are expected to be undertaken and completed.

While risk assessment and risk treatment are core risk processes, they will not be complete without the following complementary risk processes.

3. Defining the scope

Although risks relate to objectives, scope should be clearly defined and understood to give focus to the risk process.

- Strategic, operational, programme, project, or other activities?
 - Objectives and decisions, outcomes expected, time, location, specific inclusions and exclusions;
 - Risk assessment tools and techniques;
 - Resources required;
 - Responsibilities and records to be kept; and
 - Relationships with other projects, processes, and activities.
- 
- A decorative graphic in the bottom right corner consisting of a grid of blue and white squares of varying sizes, creating a pixelated or mosaic effect.

4. Defining risk criteria

Without the board or management specifying risk criteria (risk appetite or tolerance) relative to objectives, it is difficult to make risk treatment plans. To set risk criteria, the following should be considered:

- the nature and type of uncertainties that can affect outcomes and objectives (both tangible and intangible), change in customer preferences or technology obsolescence can be intangible.
- how consequences (both positive and negative) and likelihood will be defined and measured. For example they can measure in amounts or ranks or percentages or expressed using commonly agreed words.
- time-related factors. For example, seasons can influence flu and risk of excessive production of vaccines may be lowered.
- consistency in the use of measurements. For example 10 or 5-point scale.
- how the level of risk is to be determined. For example whether it will be a simple multiplication of impact and likelihood or will they be weighed based on source, for example.
- how combinations and sequences of multiple risks will be considered, meaning the extent of detail required should be specified in the manuals.
- the organization's capacity. For example treatment plans should be feasible.

5. Communication and consultation

Risks are identified and treated in teams that include all stakeholders. While inclusivity is achieved, the risk process gains quality due to expert perceptions.

6. External and internal context

Please see Appendix A1 of [Risk Framework](#).

7. Monitoring and review

It should be a planned part of the risk management process, with responsibilities clearly defined.

8. Recording and reporting

The risk management process and its outcomes should be documented and reported, considering the following factors:

- differing stakeholders and their specific information needs and requirements. For example, board reports will be more concise.
- cost, frequency and timeliness of reporting; and
- method of reporting.
- relevance of information to organizational objectives and decision-making. For example, irrelevant risks should not be reported.

[ISO 31000: 2018 gratefully acknowledged]