

Practical Tips for Conducting a Risk Assessment

Overview

This guide outlines the process for conducting a systematic risk assessment to identify, analyze, evaluate, and address risks that may impact organizational objectives. It is based on principles from [ISO 31000](#) and [COSO ERM](#), and is designed to be applied at the strategic, operational, project, or program level.

The step-by-step risk assessment process

Step 1 - Define scope and objectives

The purpose of this step is to ensure clarity on what you are assessing and why. The actions you need to take are:

Identify the area under review (e.g., entire organization, department, project)

Define the objectives of the risk assessment (e.g., regulatory compliance, strategic planning, operational continuity).

Establish boundaries; what is in scope and what is not.

Identify relevant stakeholders.

Tip: The scope should be manageable but comprehensive enough to capture key risks.

Step 2 - Establish context

The purpose of this step is to understand the environment in which the organization operates. The actions you need to take are:

Review internal context: structure, governance, policies, resources, culture.

Review external context such as market conditions, political environment, regulatory requirements, and industry trends.

Confirm risk criteria: likelihood, impact, and other measures such as velocity or controllability.

Document the organization's risk appetite and tolerance.

Tip: Context setting ensures risks are evaluated against the right backdrop.

Practical Tips for Conducting a Risk Assessment

The step-by-step risk assessment process

Step 3 - Identify risks

The purpose of this step is to capture all potential events that could impact objectives. The methods to achieve this include:

- | |
|---|
| Brainstorming workshops with cross-functional teams. |
| Environmental scanning (political, economic, social, technological, legal, or environmental factors). |
| Reviewing historical incidents, audit reports, lessons learned. |
| Interviews with key stakeholders. |

The deliverable for this step is a completed risk register with a clear description of each risk.
Tip: Phrase risks as "events that could occur" and their potential consequences not just problems.

Step 4 - Analyze risks

The purpose of this step is to understand the nature, causes, and potential consequences of each risk. The actions you need to take are:

- | |
|---|
| Assess likelihood (probability of occurrence). |
| Assess impact (effect on objectives if risk materializes). |
| Consider existing controls and their effectiveness. |
| [Optional: Factor in velocity (speed at which risk could materialize) and interdependencies]. |

Risk management tools to support this step:

- | |
|---|
| Risk matrix: with likelihood - impact matrices and qualitative scales (e.g., high/medium/low) |
| Quantitative models (e.g., financial loss estimation) |

Practical Tips for Conducting a Risk Assessment

The step-by-step risk assessment process

Step 5 - Evaluate risks

The purpose of this step is to prioritize risks for treatment. The actions you need to take are:

Plot risks on a risk matrix

Compare risk ratings against the organization's risk appetite.

Determine which risks require immediate action, monitoring, or acceptance.

Tip: Focus resources on high likelihood + high impact risks first.

Suggested risk rating scale

See here for an example 5x5 likelihood vs impact matrix:

Likelihood	Description
1	Rare
2	Unlikely
3	Possible
4	Likely
5	Almost certain

Impact	Description
1	Insignificant
2	Minor
3	Moderate
4	Major
5	Catastrophic

Practical Tips for Conducting a Risk Assessment

The step-by-step risk assessment process

Step 6 - Treat risks

The purpose of this step is to select and implement the best risk response. Treatment options include:

Avoid - eliminate the activity causing the risk.

Mitigate - implement controls to reduce likelihood/impact.

Transfer - shift the risk to another party (e.g., insurance, outsourcing).

Accept - acknowledge the risk and monitor it without additional controls.

The actions to take at this step are:

Assign responsibility for each risk treatment.

Define timelines and required resources.

Integrate risk treatments into operational plans.

Step 7 - Monitor and review

The purpose of this step is to ensure risk profile remains current and controls are effective. The actions you need to take are:

Track key risk indicators (KRIs).

Review risk registers periodically.

Conduct follow-up assessments after major changes of incidents.

Report to management and/or the Board regularly.

Tip: Continuous monitoring prevents risk blind spots.

Practical Tips for Conducting a Risk Assessment

The step-by-step risk assessment process

Step 8 - Communicate and consult

The purpose of this step is to engage stakeholders throughout the risk assessment process. The actions you need to take are:

Share risk findings with leadership and staff.
--

Involve stakeholders in indentifying and validating risks.
--

Provide risk awareness training.

Tip: Risk management works best when it's a two-way conversation, not just reporting.

Risk assessment deliverables

The deliverables you should have once you have completed your risk assessment include:

Risk register - documented list of identified risks, causes, consequences, ratings, and controls.

Risk heat map - visual representation of risks by priority.

Risk treatment plan - actions, responsibilities, and timelines.

Monitoring and reporting framework - how risk data will be tracked and reported.
--