Risk Management
Quick Reference Guide

The Seven R's and Four T's of Risk Management

PACED

Risk management is defined as a set of principles and processes that help minimize the negative impacts of risks and maximize the positive impacts.

Your risk management process should be PACED:

- **Proportionate** to the size of your organization
- **Aligned** to your organization's mission
- **Complete**
- **Embedded** into the culture of the organization and its day-to-day activities
- **Dynamic** and responsive

Establishing Your Risk Management Context

Each organization is unique, and you must identify the context in which your risk management framework must operate.

Consider:

- The regulatory or legal environment you operate in concerning internal practices (e.g. labour laws and regulations, liability claims, etc.) and how you relate to your customers and vendors.
- Communication methods you will use to notify and communicate with your stakeholders, as a range of techniques may be required to suit different stakeholder groups.
- The size of the organization in terms of the number of divisions, the revenue of business lines, size of markets, and budgets.
- Labour relations in the organization.
- The structure of the organization, which can affect risk analysis, planning, and implementation.
- The culture of the organization for risk tolerance. Is your organization a conservative family business or an edgy risk-taker?

Contingency Planning

When:

- How will we know when the risk will happen?
- What will alarms look like?
- When should we start acting?

Who:

- Who has responsibility for this risk?
- What other resources might they need?
- Who else should be informed?

What:

- What will happen when the risk occurs?
- What will we do when the risk happens?
- What consequences could the risk have?
- What other risks might this event create?

Where:

- Where is the risk going to happen?

Review Checklist

Things that should be covered in the review process include:

- Analysis of risk response measures and whether they achieved the desired result, and did so efficiently
- Review of reporting and monitoring procedures
- Knowledge gap analysis for risk assessments (Were people able to find the information they needed?)
- Compliance check with appropriate regulations and organizations
- Opinions of key external and internal stakeholders
- Self-certification
- Risk disclosure exercise to identify future risks
- A repeat of risk assessment
- Lessons learned
- Recommendations and implementation plan

The COSO ERM Cube

In 2004, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) published a risk management standard. It was designed to match up to Sarbanes-Oxley regulatory requirements for organizations in the United States and is therefore quite popular.

The cube lays out four categories of objectives at the top:

- Compliance
- Operational
- Reporting
- Strategic

This is followed by eight rows of components that are needed to achieve those objectives.

- Control Activities
- Event Identification
- Information and Communication
- Internal Environment
- Monitoring
- Objective Setting
- Risk Assessment
- Risk Response

The third dimension illustrates an organization's various business units:

- Subsidiary
- Business Unit
- Division
- Entity Level

ISO 31000 Standard/Guide 73

In 2009, the International Organization for Standardization published a guide and a standard for risk management.

ISO Guide 73 defines generic risk management terms to provide a consistent foundation for frameworks and processes. ISO Standard 31000 provides best-practice principles about risk management.

Template Components

Your organization must have a template to track and record all risk identification information. The template will vary in complexity according to your organization's needs, but basic information should include the following elements.

Basic Information

- Risk identifier, such as a number
- Date risk reported
- Who the risk was identified by

Description of Risk

- Classification
- Why is it a risk?
- Is this a hazard, opportunity, or uncertainty?
- Tangible impact (people, time, money, etc.)
- Non-tangible impact
- Data gathered or studies completed

Timeline

- When might the risk occur?
- How long could it last?
- Could it reoccur?
- What signals or alarms will we see?

Scope of Risk

- What could happen as a result of this risk?
- What is the likelihood of the overall risk and each consequence?
- What data do we have about the consequences of this risk?
- What other risks could occur from this risk?

Ratings and History

- Rate the impact (low, medium, or high) and the likelihood (likely, neutral, not likely)
- Outline previous experience with this risk
- Describe risk attitude and organizational tolerance for the risk

Existing Risk Systems:

- Existing controls and estimated effectiveness
- Monitoring procedures
- Improvement recommendations and information
- Related policy or procedural information

Types of Formal Analyses

- **SWOT:** Stands for Strength, Weakness, Opportunities, and Threats. An excellent system to create a broad picture of any situation.
- **PESTLE:** Stands for Political, Economic, Social, Technological, Legal, and Environmental. Used to assess the current market conditions and create a strategic plan.
- **HAZOP:** Stands for HAZard and OPerability study. Provides a structure and system to examine a process or operation to identify risks.
- **FMEA:** Stands for Failure Mode and Effects Analysis. A system that analyzes system failures and their effects.