Ontario

RISK MANAGEMENT STRATEGY & PROCESS TOOLKIT

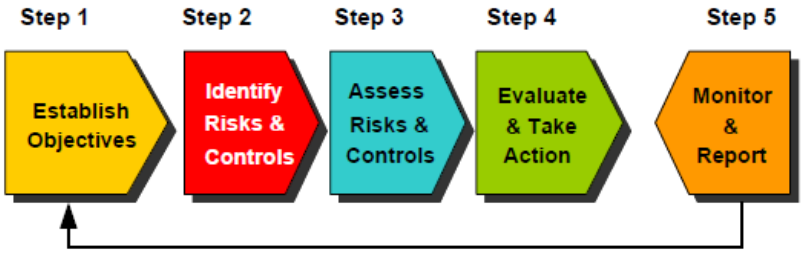
Step 1: Establish objectives

- Risks must be assessed and prioritized in relation to an objective
- Objectives can be at any level; operational, program, initiative, unit, branch, health system
- Each objective can be general or can include specific goals, key milestones, deliverables and commitments

Risk
The future event that may impact the achievement of established objectives. Risks can be positive or negative.

Control / Mitigation Strategy
Controls / mitigation strategies reduce negative risks or increase opportunities.

The risk management process



Consequences
- Identify the specific consequences of each risk
- Consider financial, non-financial, performance, etc.

Vulnerability
- Identify exposure to risk
- Vulnerability may vary with each situation and change over time

Cause/Source of Risk
- Understand the cause/source of each risk
- Use a fish-bone diagram

Step 2: Identify risks & controls

Identify risks - What could go wrong?
- Consider each category of risk
- Obtain available evidence
- Brainstorm with colleagues and/or stakeholders
- Examine trends and consider past risk events
- Obtain information from similar organizations or projects
- Increase awareness of new initiatives/ agendas and regulations

Identify existing controls – What do you already have in place?
- Preventive controls
- Detective controls
- Recovery / Corrective controls

14 categories of risk

RISK	Description
Financial	Uncertainty around obtaining, committing, using, losing economic resources; or not meeting overall financial budgets/commitments.
Operational or Service Delivery	Uncertainty regarding the activities performed in carrying out the entity's strategies or how the entity delivers services.
People / Human Resources	Uncertainty as to the capacity of the entity to attract, develop and retain the talent needed to meet the objectives.
Environmental	Uncertainty usually due to external risks facing an organization including air, water, earth, forests. . An example of an environmental, ecological risk would be the possible occurrence of a natural disaster and its impact on an organization's operations.
Information / Knowledge	Uncertainty regarding access to, or use of, inaccurate, incomplete, obsolete, irrelevant or untimely information; unreliable information systems; inaccurate or misleading reporting.
Strategic / Policy	Uncertainty around strategies and policies achieving required results; or that old and/or new policies, directives, guidelines, legislation, processes, systems, and procedures fail to recognize and adapt to changes.
Legal / Compliance	Uncertainty regarding compliance with laws, regulations, standards, policies, directives, contracts, MOUs and the risk of litigation.
Technology	Uncertainty regarding alignment of IT infrastructure with technology and business requirements; availability of technological resources.
Governance / Organizational	Uncertainty about maintenance or development of appropriate accountability and control mechanisms such as organizational structures and systems processes; systemic issues, culture and values, organizational capacity, commitment, and learning and management systems, etc.
Privacy	Uncertainty with regards to exposure of personal information or data; fraud or identity theft; unauthorized data.
Stakeholder / Public Perception	Uncertainty around managing the expectations of the public, other governments, Ministries, or other stakeholders and the media to prevent disruption or criticism of the service and a negative public image.
Security	Uncertainty relating to breaches in physical or logical access to data and locations (offices, warehouses, labs, etc).
Equity	Uncertainty that policies, programs, or services will have a disproportionate impact on the population.
Political	Uncertainty that events may arise from or impact the Minister's Office/Ministry, e.g. a change in government, political priorities or policy direction.

Ontario

RISK MANAGEMENT STRATEGY & PROCESS TOOLKIT

Step 3: Assess Risks & Controls

Assess inherent risks

- *Inherent likelihood* – Without any mitigation, how likely is this risk?
- *Inherent impact* – Without any mitigation, how big will be the impact of the risk on your objective?

Assess controls

- Evaluate possible preventive, detective, or corrective mitigation strategies.

Reassess residual risks

- Re-assess the impact, likelihood and proximity of the risk with mitigation strategies in place.
- *Residual likelihood* – With mitigation strategies in place, how likely is this risk?
- *Residual impact* – With mitigation strategies in place, how big an impact will this risk have on your objective?

Key Risk Indicators (KRI)

- Leading Indicators - Early or leading indicators that measure sources or causes to help prevent risk occurrences
- Lagging Indicators - Detection and performance indicators that help monitor risks as they occur.

Risk Tolerance

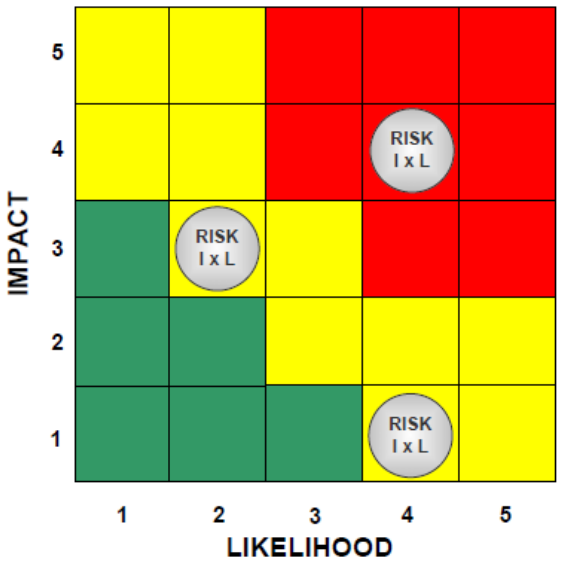
- The amount of risk that the area being assessed can manage

Risk Appetite

- The amount of risk that the area being assessed is willing to manage

The tolerance and risk appetite values may differ e.g. Staff can afford to lose email capabilities for five hours (risk tolerance) but only be willing to lose email capabilities for one hour (risk appetite).

RISK PRIORITIZATION MATRIX



Step 4: Evaluate & Take Action

- Identify risk owners.
- Identify control owners.
- Have mitigation strategies reduced the risk rating (Impact x Likelihood) enough that the risk is below approved risk tolerance levels?
- Do you need to implement further mitigation strategies?
- Develop SMART (Specific, Measurable, Achievable, Realistic, Time-specific) actions that will either reduce the likelihood of the risks or minimise the impact.
- Develop detailed action plans with timelines, responsibilities and outline deliveries.

Step 5: Monitor & Report

- Have processes in place to review risk levels and risk mitigation strategies as appropriate.
- Monitor and update by asking:
  - Have risks changed? How?
  - Are there new risks? Assess them
  - Do you need to report or escalate risks? To whom? When? How?
- Develop and monitor risk indicators

Definitions

VALUE	LIKELIHOOD	IMPACT	PROXIMITY	*SCALE*
1	Unlikely to occur	Negligible Impact	More than 36 months	*Very Low*
2	May occur occasionally	Minor impact on time, cost or quality	12 to 24 months	*Low*
3	Is as likely as not to occur	Notable impact on time, cost or quality	6 to 12 months	*Medium*
4	Is likely to occur	Substantial impact on time, cost or quality	Less than 6 months	*High*
5	Is almost certain to occur	Threatens the success of the project	Now	*Very High*