Board of Health Manual
Public Health Sudbury & Districts

Policy

Category
Board of Health Structure & Function

Section
Management

Subject
Enterprise Risk Management

Number
C-III-12

Approved By
Board of Health

Original Date
October 20, 2016

Revised Date
June 21, 2018

Review Date
June 21, 2018

Purpose
Public Health Sudbury & Districts shall have a risk management framework based on a risk management process developed by the Ontario Internal Audit Division of the Treasury Board Secretariat. The framework will ensure risks are identified and will ensure that monitoring and response systems are in place at Public Health Sudbury & Districts to effectively respond to these risks.

The Board of Health shall set the tone that systematic, integrated risk management is valuable for managing risks and for demonstrating accountability to stakeholders.

The Board of Health supports the following principles:

- Risk management is an essential component of good management.
- Risk management is imbedded into the culture and operations of the health unit.
- Better decisions are made when supported by a disciplined approach to risk management.
- Risk management activities should be aligned with strategic objectives at all levels of the organization.

- Risk management should be integrated into informed decision making and priority setting and should become part of day-to-day management activities.
- Threats should be managed and opportunities leveraged as appropriate and in accordance with best practices.
- The agency's risk should be re-assessed regularly and risk and mitigation strategies should be reported on regularly.
- Through the risk management process, the agency should anticipate and respond to changing social, environmental and legislative requirements.
- The integration of risk management into decision making should be supported by a corporate philosophy and culture that encourages everyone to manage risk and to communicate openly about risk.
- Every employee has a role to play in risk management.

Process:

The Board of Health approves the risk management framework (see Appendix A) and establishes its risk appetite in relation to specific risks. These are documented in the Risk Management Risk Assessment and Heat Map (see Appendix B).

The Board receives and reviews an annual report of risks and mitigation strategies of currently identified risks. A comprehensive risk management review will occur every three years to ensure that identified risks are still relevant to the organization and reflective of community and political contexts.

Definitions:

Risk: Risk is an uncertain event or condition that, if it occurs, has an effect on the achievement of objectives. It includes both threats to the objectives and opportunities to improve on the objectives Adapted from Project Management Institute PMBoK 2000

Enterprise Risk Management: A holistic and integrated risk management process that takes a strategic view of risk across the whole organization or enterprise.

Risk Management: A systematic approach to setting the best course of action under uncertainty by identifying, understanding, acting on, monitoring and communicating risk issues.

Risk Appetite: The amount and type of risk that the organization is willing to take in order to meet strategic objectives.

Risk Management Framework: Establishes a process for implementation of effective risk management practices at all levels of the organization. The Public Health Sudbury & Districts Risk Management Framework, which follows the five step risk management process developed by the Treasury Board Secretariat, articulates a five-step approach to risk management which provides the flexibility to manage risks accordingly.

Risk Management Plan: The organization's risk management plan includes the implementation of effective risk management processes and strategies to actively respond to change and uncertainty in a timely manner and to demonstrate accountability to stakeholders.

Appendix A: Public Health Sudbury & Districts' Risk Management Framework

Summary

The purpose of this risk management framework is to establish a process for implementation of effective risk management practices at all levels of the organization. This framework, which follows the five step risk management process developed by the Treasury Board Secretariat, articulates a five-step approach to risk management which provides the flexibility to manage risks accordingly.

The risk management policy is aimed at fulfilling risk management requirements set out within the 2018 Ontario Public Health Standards' Organizational Requirements.

Philosophy Statement

Public Health Sudbury & Districts is committed to fostering an environment that supports a continuous quality improvement approach to organizational effectiveness. This includes the implementation of effective risk management processes and strategies to actively respond to change and uncertainty in a timely manner and to demonstrate accountability to stakeholders.

Background

Public Health Sudbury & Districts acknowledges that there is an element of risk in any decision or activity and risk taking may be deemed acceptable when appropriately managed. Risk is defined as:

> Risk is an uncertain event or condition that, if it occurs, has an effect on the achievement of objectives. It includes both threats to the objectives and opportunities to improve on the objectives.
>
> Adapted from Project Management Institute PMBoK 2000

The 2018 Ontario Public Health Organizational Requirements mandate Board of Health stewardship and oversight of risk management. The Medical Officer of Health, and through delegation to all staff, has the responsibility to monitor and respond to emerging issues and potential threats to the organization. Potential threats include but are not limited to; financial, human resources, operational, technology and legal risks.

SDHU Risk Management Framework*

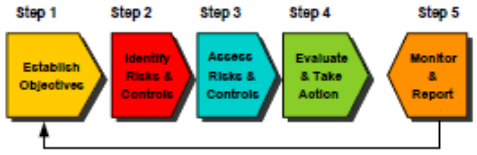
Step 1: Establish objectives

- 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

*Based on the Risk Management Strategy & Process Toolkit from the Ontario Internal Audit Division, Treasury Board Secretariat

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.

SDHU Risk Management Framework

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?

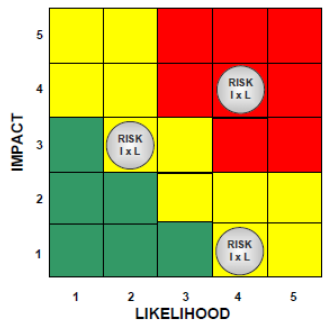
Key Risk Indicators (KRI)
- Leading Indicators - Early or leading indicators that measure sources or causes to help prevent risk occurrences
- Lagging Indicators - Detection and performance indicators that help monitor risks as they occur.

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

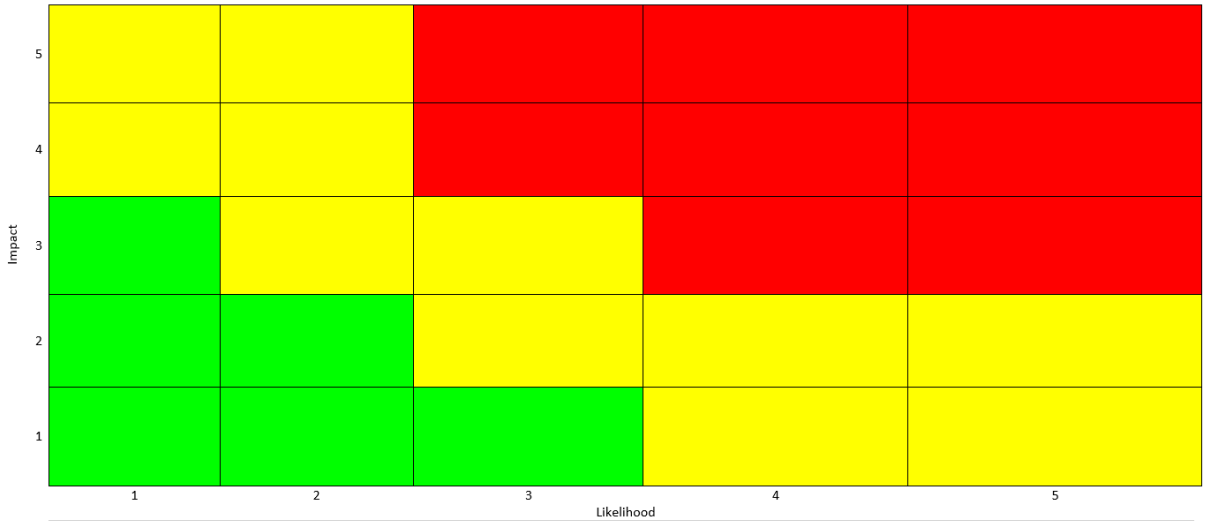
Definitions

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*

Appendix B: Public Health Sudbury & Districts Organizational Risk Assessment and Heat Map

Public Health Sudbury & Districts Organizational Risk Assessment	
Overall Objective:	
Subordinate Objective:	
Risk Categories	Rating Scale
1. Financial Risks	
2. Governance / Organizational Risks	
3. Human Resources	
4. Knowledge / Information	
5. Technology	
6. Legal / Compliance	
7. Service Delivery / Operational	
8. Environment	
9. Political	
10. Stakeholder / Public Perception	
11. Strategic / Policy	
12. Security Risks	
13. Privacy Risks	
14. Equity Risks	

Organizational Risks: Heat Map of Current Residual Risks



Low Risk	Risks do not exist or are of minor importance and are not likely to significantly affect the achievement of objectives. Risks can be managed by routine procedures.
Medium Risk	Risks are a moderate threat to the achievement of objectives. Specific management responsibilities and specific procedures are required.
High Risk	Risks are a significant threat to the achievement of key objectives. Detailed management planning and attention is required.