association of family health teams of ontario

RISK MANAGEMENT:

A Toolkit for AFHTO Members

TABLE OF CONTENTS

A. INTRODUCTION 2
Purpose of This Document 2
Contents 2
How to Use This Document 2
B. OVERVIEW 3
What is Risk Management 3
Defining Key Terms 3
C. MOHLTC-FHT CONTRACT REQUIREMENTS 4
D. OVERVIEW OF RISK MANAGEMENT 4
Domains of Risk 4
Essential Components of Risk Management 5
Typical Risk Management Process 5
E. RISK MANAGEMENT AND THE BOARD 6
Role of the Board in Risk Management 6
Establishing Management Accountability 7
Effective Governance is Essential to Managing Risk 7
Organizing for Board Leadership on Risk 8
1. Board Committees 8
2. Board Policies 9
3. Insurance 10
APPENDIX A: Sample Risk Framework 11

A. INTRODUCTION

Purpose of This Document

This document is designed for use by AFHTO member Boards to support learning and fulfillment of the Board's role in overseeing the effective management of risk in their organization.

Contents

The document includes the following:

- definition of risk management and other key terms;
- a list of requirements related to risk management in the Ministry of Health and Long-Term Care (Ministry)-Family Health Team (FHT) contract and attestation document;
- an overview of risk management including domains of risk, the key components that make up a risk management approach, and the steps in a standard risk management process;
- a description of the Board's role in risk management and common governance practices for the Board to fulfill this role; and,
- sample tools and links to other reference materials for use in developing a risk management approach in your organization.

How to Use This Document

The following are suggested steps for using this document:

1. Review the complete document.
2. Consider your own Board's current understanding if risk management and the current policies, structures and processes in place in your organization. Together with the Board and CEO/ED, discuss whether there are any gaps in knowledge, process or practice that need to be addressed and the actions to be taken to address them. This is particularly important if your organization is a FHT and there are gaps in meeting the new contract and attestation requirements.
3. Consider setting out Board expectations for risk management including assigning responsibility and Board-required oversight processes to be followed.
4. If you have any feedback on this toolkit, including suggestions to improve its contents, contact:

Bryn Hamilton, Provincial Lead
Governance and Leadership Program
Email: bryn.hamilton@afhto.ca
Direct Phone: 705-321-7580

B. OVERVIEW

What is Risk Management

No organization or individual functions without taking some level of risk in the activities they perform every day, constantly distinguishing between risks that create positive impact and opportunities for growth from those that are excessive and may lead to negative outcomes. Risk management is the process of identifying, analyzing, acting on and mitigating where needed the risks that arise in many different activities. Within an organization specifically, risk management is a set of established and systematic processes, actions and decisions that together ensure that risks are identified, assessed and responded to at all levels within the organization.

Identifying and managing risk is well recognized as one of the primary roles of a Board. A Board faces two challenges in operationalizing this role. First, risk management cuts across virtually every aspect of Board activity and decision-making so needs to be embedded across a wide range of the Board's processes and tools, rather than in a single policy or decision. The second challenge for a Board is balancing its responsibility for effective risk management with its overall responsibility to ensure organizational success and sustainability, goals which inherently involve taking risks. The Board needs to ensure proper management of risks while not becoming so focused on risk that it holds the organization back from reaching its full potential for success.

The intent of this toolkit is to provide an overview of what a Board needs to know about and do to fulfill its responsibilities related to risk management and risk oversight.

Defining Key Terms

There are several key terms in the discussion of organizational risk management:

- **Risk**, simply stated, is any factor that could have an impact on the organization either positively or negatively. It refers to any uncertainty in achieving the organization's objectives or the uncertainty that surrounds future events and outcomes. These uncertainties may be related to the **likelihood** of the event occurring, the expected frequency of the event, and the severity of the **impact** if the event occurs.
- **Risk Management** refers to the identification, assessment, and processes and strategies put in place to help the organization mitigate the adverse effects of such risks.
- **Enterprise Risk Management**, or ERM, refers to a comprehensive risk management framework used by the organization to identify, assess and manage risks across the entire organization with the intent of enhancing the organization's success and sustainability. It captures all types of risks facing the organization (e.g., operational, financial, reputational) and in health care organizations it includes both clinical and non-clinical risks. ERM is a proactive rather than reactive approach that includes structured, continuous assessment of risk, clear accountabilities and roles related to risk, and clear and purposeful communication within the organization and with external stakeholders. The overall goal of ERM is to enhance the likelihood of the organization's success and support a high level of stakeholder trust and confidence in the organization.

C. MOHLTC-FHT CONTRACT REQUIREMENTS

The Ministry-FHT Contract, and accompanying Attestation Template for 2018-2019, includes the following requirements related to risk management:

Ministry-FHT Contract	Reference
Risk Management as a Board Skill • The FHT is required to use its best efforts to ensure that its Board possesses skills in certain specified areas, one of which is Risk Management.	Schedule A, Appendix 1
Risk Management on the Board Skills Matrix • "Risk Management" is listed on the Board Skills Matrix provided with the Contract and FHTs are required to indicate the skill level of each Board member.	Schedule A, Appendix 2
Compliance Attestation Template	Reference
Annual Submission of Risk Management Plan • The FHT is required to submit a copy of the Risk Management Plan with the annual Attestation document.	Attestation Template, Page 3
Confirmation of Risk Management Plan • The FHT is required to indicate that it has a current Risk Management Plan and, if not, to provide an explanation.	Attestation Template, Item 25

D. OVERVIEW OF RISK MANAGEMENT

While it is not the Board's role to develop or manage the organization's day-to-day risk management practices, fulfilling its own governance responsibilities in this area requires the Board to have a good understanding of the key components and best practices in risk management. This section provides an overview of the key elements of a risk management program.

Domains of Risk

Risks are normally categorized along a small number of overall dimensions, categories or domains. There is no one correct way to group the risk domains, what matters is that all domains relevant to the organization are captured. In its discussion of risk management, *AFHTO Fundamentals of Governance* identifies five general categories of risk: clinical, strategic, operational, financial, compliance, and reputation.

Another approach is shown in the diagram in Appendix A. It provides a detailed illustration of how risks for a health-care organization can be grouped into three main categories - business risk, resource risk, and compliance risk – with sub-groups of risks further identified within each category.

Essential Components of Risk Management

There are three general components in a comprehensive risk management program all of which are captured in the organization's risk management plan:

- **Preparation -** This involves identifying and periodically reviewing risks, assessing each risk in terms of its likelihood of occurrence and potential impact on the organization, and determining how to respond to the risk (e.g., avoid, accept, reduce likelihood, or plan for occurrence).
- **Prevention** - This involves ensuring the risk management plan is implemented as required and along with strategies for prevention and/or mitigation of specific risks. Strategies include:
  - establishing and implementing operational policies and procedures for avoiding risk, monitoring for potential risk, and taking corrective action when needed,
  - educating staff about policy, procedure and actions to take in the event of a risk occurring; and,
  - building a proactive organizational culture that includes understanding and identifying risks when they occur, and a "no-blame" approach where staff are comfortable speaking up.
- **Protection** – This involves taking proactive steps to mitigate the effect of risks on the organization through various means including purchasing insurance, establishing contractual protections against risks, and establishing contingency plans to diminish the impact of risks and surprise events when they do occur, such as emergency preparedness for disasters and patient occurrences.

Typical Risk Management Process

Risk management is a disciplined process that typically unfolds in a sequence of structured activities divided into specific phases, with each phase building on the previous one. The process below describes the generally accepted progression of activities involved in risk management. It includes five phases but the activities can be combined into fewer or additional phases as needed.

1. **Building Context** – This includes:
   a. committing and getting buy-in to the project
   b. identifying the core risk management team
   c. selecting or developing a risk management framework
   d. creating a project plan/project charter.
2. **Risk Identification** - This includes:
   a. identifying sources of risk
   b. identifying each risk that may arise
   c. grouping the risks where possible or relevant
   d. identifying sources of risk identification.
3. **Risk Assessment** – This includes:
   a. classifying risks into groups

   b. assessing the likelihood of each risk and its potential impact on the organization
   c. mapping risks onto a risk assessment matrix or tool.
4. **Risk Response** – This includes:
   a. identifying the types of response for each potential risk
   b. where there are several response options, evaluating the potential options (e.g., avoid, mitigate, respond, share) and identifying the preferred option
   c. allocating responsibilities for monitoring and responding to each risk
   d. implementing the risk response as needed.
5. **Monitor and Sustain** - This includes:
   a. continuous checking, supervising, critically observing, and determining the status of potential and real risks
   b. maintaining a database of risks and responses
   c. regularly monitoring the effectiveness of risk management practices and responses, and compliance with established policies and procedures
   d. evaluating and updating the risk management framework as needed.

A tool for use in steps 2, 3 and 4 is available in the AFHTO Governance Fundamentals Toolkit: the "Sample Risk Management Matrix"

E. RISK MANAGEMENT AND THE BOARD

Role of the Board in Risk Management

Risk management is one of the primary roles of the Board. As with other aspects of governance, the Board is responsible for establishing policy, making decisions that are beyond the authority of staff, and overseeing the management of risk. While a Board may delegate to management much of the work related to risk management, is cannot delegate its responsibility for oversight of risk.

There are three parts to the Board's role related to risk:

- **Establishing a risk-aware culture** – As with all parts of the organizational culture, creating a risk-aware culture starts at the top. The Board does this by making, and being seen to make, risk awareness and risk management a priority in its ongoing work.
- **Ensuring a proactive and comprehensive approach to risk** - The Board sets the requirements for all aspects of risk management in the organization and holds the organization and each other (through Board evaluation) accountable for fulfilling those requirements.
- **Continuous monitoring and learning** – The Board ensures that risk management is part of the organization's ongoing drive to achieve its Mission through continuous learning and quality improvement.

As noted earlier, specific Board responsibilities related to risk cut across all aspects of the Board's activity and decision-making. A detailed list of Board responsibilities, including those specifically related to risk management, is found in the Board Role Checklist available to AFHTO members.

An informative resource on the Board's role in risk management is "20 Questions Directors Should Ask About Risk" by the Canadian Institute of Chartered Accountants. This document is referenced in *AFHTO Governance Fundamentals* and is available here. Another useful resource created for health care Boards is found here.

Establishing Management Accountability

As with other aspects of the organization's operations, the Board delegates much of the responsibility for effective risk management to the CEO/ED and uses formal mechanisms to:

- **delegate authority for risk management** to the CEO/ED (in the CEO/ED job description, a formal delegation of authority policy, and/or a CEO/ED role policy)
- **define performance expectations for risk management** (in the CEO/ED's annual performance goals) and
- **monitor achievement of expectations** (in the annual EO/ED performance review).

In addition, the Board needs to assure itself that management has in place the appropriate policies, processes, plans and programs to fulfill the Board's requirements and to prepare for, prevent, and protect the organization from foreseeable and material risks.

One of the more specific mechanisms for the Board to do is in approving the organization's Risk Management Plan developed by management. The Plan usually sets out how the organization will prevent and protect itself from risks, and how it will address risks that occur. By reviewing and approving this plan the Board is informed about how management expects to fulfill its specific risk management responsibilities and enables the Board to hold management accountable for what it includes in the plan. As noted earlier, each FHT is required to submit this plan to the Ministry with their annual compliance attestation.

Effective Governance is Essential to Managing Risk

Oversight of management alone is not sufficient to fulfill the Board's own obligations for managing risk. The Board and every Board member must know their responsibilities, have the skills and information needed to fulfill them, and act in a way that is consistent with the risk management needs of the organization.

Requirements for proper Board management of risk go to the very heart of effective governance and include the following:

- **Clear Board and committee accountability** – the Board and each committee must be clear on its functions related to risk management and have the skills to perform them. This includes:

- Ensuring committees involved in risk management have clearly defined mandates, reporting requirements and list of functions related to risk management, as well as committee members with appropriate skills.
- Orienting Board and committee members about risk management and providing ongoing education as needed;
- Ensuring Board members recognize and act based on their independence to perform their duties including asking questions of the Board and committees, keeping free of external influences, and requesting independent advice when it is thought to be needed.

- **Quality information and advice** - To discharge their responsibilities for risk management, Board members rely on quality information from a number of sources including management reports that are appropriate and understandable, advice/reports from clinical or technical experts within the organization, and advice/reports from external sources as appropriate. The Board needs to use its common sense regarding the completeness and accuracy of information it receives and be prepared to request verification and/or additional information and advice when it determines the need, before taking any action.
- **Active participation in key oversight processes** – Board members need to be active and informed participants in processes established to plan and manage key aspects of the organization to protect against risk. Processes related to financial and quality oversight are particularly critical.
- **Decisive action in response to identified risks –** Being skilled and responding is not enough to ensure risks are properly managed. Every Board member, and the Board as a whole, must be prepared to make decisions and act when the information before them indicates a significant risk to the organization. This includes:
  - Questioning the reasonableness of assumptions and the potential risks to execution of plans presented by management;
  - Questioning the level of preparedness of management for implementation of the plan and for contingencies and unexpected events;
  - Taking Board action or directing management to respond in exceptional circumstances when events or information emerge that pose risks for the organization.

Organizing for Board Leadership on Risk

1. Board Committees

To support the Board's overall responsibility for risk management, Boards look to their committees for more detailed oversight and management of risk. Some Boards have a dedicated Enterprise Risk Management Committee or add risk management responsibilities to the mandate of an existing standing committee (e.g., Board Committee on Quality and Risk). Since risks arise across all aspects of committee work, however, many Boards prefer to assign the pertinent aspects of risk management to each Board committee. With this approach, responsibilities may be assigned as follows:

- **Program or Quality Committee** – reviews program effectiveness, quality assurance and quality management programs related to risks and contingencies;

- **Finance Committee** – reviews financial condition risks including adequacy of the budget, efficiency related to funding, simulations and sensitivity to revenue shortfalls, adequacy of financial reporting and controls, and the need for insurance;
- **Audit Committee** (may be combined with Finance above) – reviews adequacy and implementation of risk management policies related to the integrity of key processes and information; and,
- **Governance Committee** – reviews Board policies and practices related to risk management including ensuring risk management policies are kept up to date and Board evaluation includes an evaluation of the Board's fulfillment of its risk management responsibilities.

2. Board Policies

Board-approved policies are a key mechanism for the Board to establish clear expectations and accountabilities for the whole organization related to risk management. Board policies on risk management are seen as a way ensure proper protection of assets and compliance with legal requirements. While those goals are vital, strong Board policies are an essential part of protecting people (including staff and the community served), the organization's reputation, and its future ability to achieve its mission.

Board policies should go beyond basic protections to also establish clear accountabilities, define the organization's tolerance and capacity for specific types of risk, and provide a foundation for overall risk management that enables the organization to deal with ongoing risks (and opportunities) and weather unexpected setbacks. Board policy related to risk can be in the form of risk-specific policies (such as a policy on cyber risk) or through integrating risk-related content into a general Board policy (such as a policy on procurement). As such, there is no single list of recommended Board policies on risk – rather, each organization should determine the policies it needs and how to arrange the information across the various Board and organizational policies.

Finally, the following can be kept in mind when developing a Board policy framework on risk:

- Thoughtful development of risk management policies can be a lengthy process because it requires a broad assessment and decisions on many aspects of organizational process and many different roles/accountabilities.
- There should be an overall discussion of the organization's approach or philosophy about risk. Does it operate from a risk-tolerant or risk-averse standpoint, or somewhere in between? The benefits and challenges to each option can be considered and the conclusion should be a mutually-agreed approach that is articulated in writing in Board policy.
- An essential question to ask throughout is what should be included in Board policy and what goes into operational policy for which the CEO/ED is accountable.
- Sample policies from other organizations are useful background to understand different approaches and language, but policies should reflect your own organization's unique operating environment, priorities and external environment.

- Keep the Mission in mind when evaluating risk and defining how the organization will manage risk. Attempting to eliminate risk altogether, while being almost impossible, may also prohibit the organization from effectively fulfilling its mission because risk is inherent in most opportunities for change and growth.

3. Insurance

Insurance coverage is often one of the first things organizations look at when establishing a risk framework. There are many types of insurance to be considered including general liability insurance, Directors' and Officers' insurance, commercial property, and workers' compensation.

The Board should understand what types of insurance are in place for the organization, and ensure that coverage is appropriate and premium payments are up-to-date. The Board does this by holding the CEO/ED accountable for having appropriate insurance protection in place, proper maintenance of the organization's insurance program, and requiring regular written confirmation from the CEO/ED on compliance with any insurance requirements.

APPENDIX A: Sample Risk Framework

BUSINESS RISK
Risks related to the delivery of care incuding internal and external factors that may impact operations.

- **QUALITY CARE AND PATIENT SAFETY**
  Risks that the delivery of quality care is compromised and may result in an adverse outcome to the patient.
- **CORPORATE GOVERNANCE**
  Risk that the organization structure, decision-making processes, Board processes and practices do not support the startegic dirction of the organization.
- **OPERATIONS AND BUSINESS SUPPORT**
  Risk that business operations do not effectively and efficiently support the needs of the organization, its staff and patients.
- **REPUTATION AND PUBLIC IMAGE**
  Risks that the organization's reputation or image is negatively affected by issues such as patient satisfaction, media exposure and external relationships.

RESOURCE RISK
Risks related to the resources used by the organization to accomplish its objectives.

- **HUMAN RESOURCES AND STAFF/PERSONNEL RELATIONS**
  Risks associated with employment and other relationships with staff, and associated and affiliated personnel.
- **FINANCIAL**
  Risks associated with sufficiency of capital and operating funding and ineffective financial management and reporting.
- **INFORMATION,SYSTEMS AND TECHNOLOGY**
  Risks arising from technology and data including unreliability, improper use and insufficient protection, such as for cyber security.
- **PHYSICAL ASSETS**
  Risks related to the acquisition, maintenance and disposal of the organization's physical assets including buildings and equipment.

COMPLIANCE RISK
Risks related to requirements to comply with regulation, legisation, policies, directives or legal agreements.

- **ENVIRONMENT, HEALTH AND SAFETY**
  Risks related to a providing a safe environment for staff, patients and the public. The risk of not being environmentally friendly.
- **LEGAL AND REGULATORY**
  Risk that the organization is exposed to undue liability as a result of non-compliance with legislation, contractual agreements and regulatory standards.
- **POLICY**
  Risk of non-compliance with established direction and requirements established in approved policies, guidelines, directives, both internal and external to the organization.
- **STANDARDS**
  Risk of non-compliance with established accreditation standards and those requirements of the applicable professional regulatory bodies and standards committees.

The above is adapted from a framework described “Risk Management in Child and Youth Mental Health” a resource guide created by the Ontario Centre of Excellence for Child and Youth Mental Health. The full document is available at:
http://www.excellenceforchildandyouth.ca/sites/default/files/resource/guide_risk_management.pdf