HOPA

Growing in Strength
The Reciprocal Advantage

ENTERPRISE RISK MANAGEMENT FRAMEWORK

June 2022

Mission

Our mission is to provide sustainable comprehensive risk management products and services to support our members in achieving their quality and safety aims.

Vision

Our long-term vision is to be the preferred provider of strategic insurance and risk management solutions for public and private health care organizations in Atlantic Canada.

Values

In carrying out our mission, HOPA's Board, staff and volunteers will strive to be:

Member-focused—with programs and services that proactively support and add value to our members' risk management efforts;

Solution-oriented—with innovative and practical tools and approaches that are affordable and responsive to the changing risk management needs of our members;

Informed—with an emphasis on best practice and evidence-based decision-making; and

Accountable—with member communication and engagement practices that foster trust and confidence in our organization and its direction.

Contents

1 Executive Summary

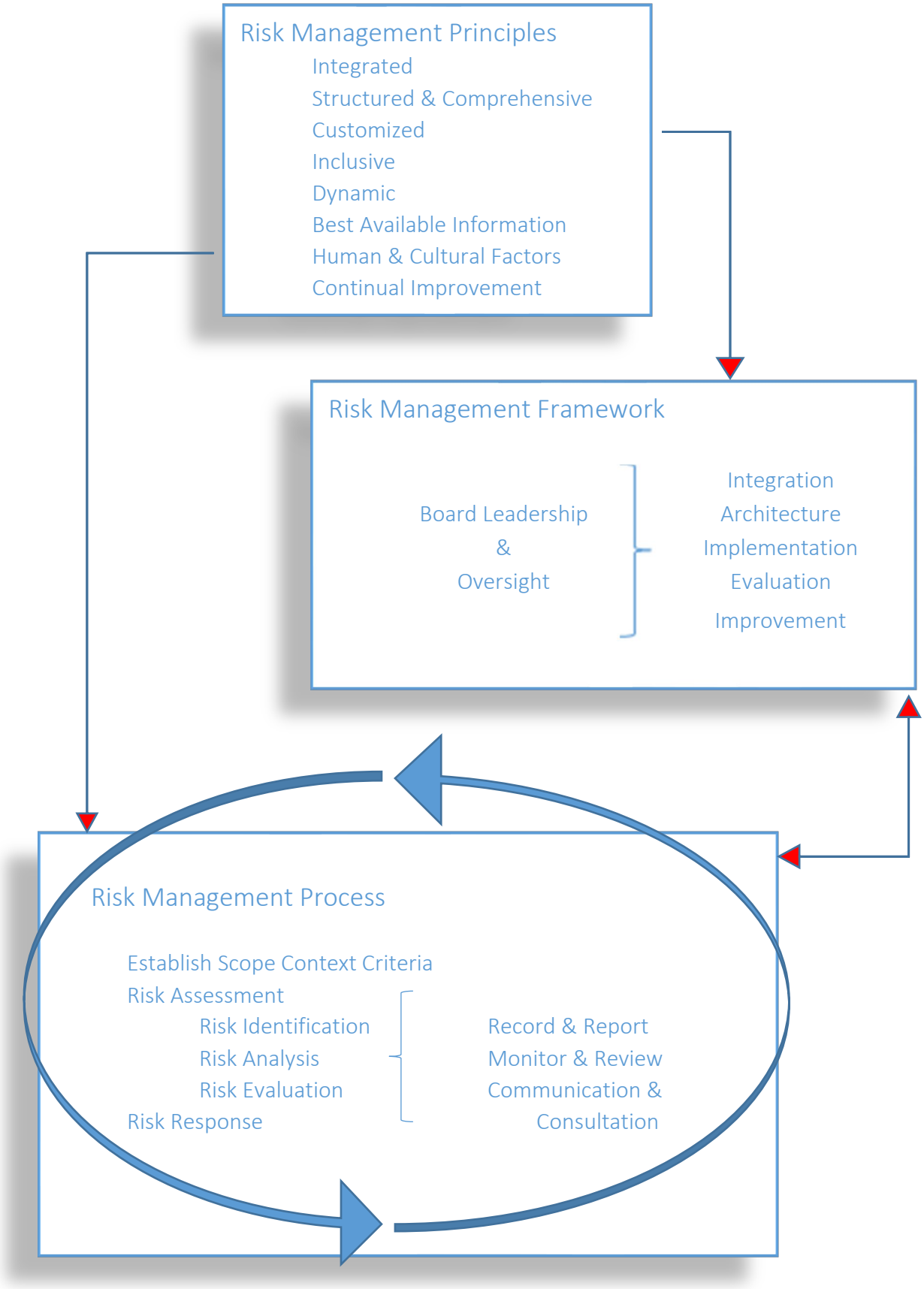
The Health Organizations Protective Association (HOPA) is committed to implementing and maintaining an enterprise risk management program to support the creation and protection of value and the achievement of HOPA's objectives. HOPA is committed to providing comprehensive risk management products and services for our subscribers.

Risk is defined as the effect of uncertainty on objectives. The purpose of the Enterprise Risk Management Framework (the Framework) is to outline our approach to understanding and managing risk to ensure it is efficient, effective and appropriate for HOPA's level of risk and responsiveness to changing the risk environment. The Framework represents HOPA's commitment to embedding effective enterprise risk management practices in governance and operational activities, and to the continuous review and improvement of enterprise risk management processes in response to change.

> *It is not the strongest or the most intelligent who will survive but those who can best manage change. – Charles Darwin*

The Framework is an important governance and management tool to ensure that HOPA continues to successfully provide sustainable and comprehensive risk management products and services to support our members in the achievement of their quality and safety aims.

1.1 ISO 31000 Risk Management Principles, Framework and Processes



2 Overview

Enterprise risk management (ERM) has been described as the discipline, culture and control structure that drives improvement of our management of risk in a changing business environment.[1] A robust ERM framework enables HOPA, as a reciprocal insurer, to better identify, measure, accept, control, report and monitor all material risks.[2] To be effective, the ERM framework must be embedded in business operations, and aligned with our corporate culture and strategic goals.[3]

The objective of ERM is to identify, assess and manage risks that have the potential to:

- negatively impact the achievement of objectives, or
- be exploited to enhance the achievement of objectives.

ERM also provides a reliable process for informed decision-making to assess and the prioritization of alternative courses of action. It protects against long-term under performance, supports a risk aware culture and strengthens board and senior leadership alignment on key issues facing HOPA.

The ERM Framework sets out the process for the assessment of risk, selection of response options and the monitoring and reporting of results. It is based on a set of underlying principles that inform the design of the risk assessment process. As the ERM Framework is applied and evaluated, HOPA's ERM expertise will grow as will the value of ERM as a tool in developing an integrated view of risk and an understanding of the upside and downside of strategic and operational decisions.

2.1 Overarching Principles

There are eight overarching principles to ensure effective, efficient, and consistent enterprise risk management.[4]

1. Customized & Proportionate – The assessment of risk is undertaken in the context of HOPA's objectives and with a deep understanding of the internal and external context in which HOPA operates. ERM activities will be proportionate to the complexity of the risk faced by HOPA and customized to fit the scope of the activity under review.

[1] What is ERM and Why is it Important? Jim Deloach Corporate Compliance Insights, June 30, 2018
[2] Enterprise Risk Management for Insurers Oct 2015. TorontoCentre: Global Leadership in Financial Supervision p 3
[3]
[4] ISO 31000:2018(E)

2. Structured & Comprehensive – HOPA's approach to ERM will be consistently applied and, to the extent possible, measurable criteria will be used to assess risk and to measure the effect of risk mitigation strategies. This will ensure that there is a reliable basis on which to monitor and evaluate the effectiveness of ERM activities and to identify when it is appropriate to adjust our processes and strategies to adapt to changing conditions.

3. Inclusive – Timely involvement of internal and external stakeholders is important to ensure that their knowledge, views and perceptions inform the ERM process and informs our approach to shared risks. Inclusivity is an important aspect of a risk aware culture and embedding ERM throughout the Association.

4. Integrated - ERM is a responsibility of the board, senior leadership and staff. It is an integral part of all organizational activities, embedded in decision making processes and aligned with the governance, management and organizational processes.

5. Dynamic - ERM must be dynamic and responsive to emerging and changing risks.

6. Best Available Information - ERM processes require comprehensive information from varying internal and external sources and should explicitly consider any limitations of available information.

7. Human & Cultural Factors - Human and cultural factors influence all aspects of ERM and must be a consideration in the evaluation of and response to risk.

8. Continual Improvement – How we understand and manage risk is improved through learning and experience, and resources must be committed to the continual improvement of the ERM program as it matures over time.

3 Enterprise Risk Management Process

The ERM process involves the systematic application of HOPA's policies, procedures and practices for the purpose of effectively managing risk. A defined process helps to ensure that ERM activities are effective in the mitigation or exploitation of the impact of risk on the achievement of HOPA's objectives, and protect against long term underperformance.

Although the risk management process is often presented as sequential, in practice it is iterative.

ERM process includes the following steps:

1. establish the ERM scope and context
2. establish the risk criteria
3. conduct the risk assessment, including;
    a. risk identification
    b. risk analysis; severity and likelihood
    c. risk rank
4. consider risk response strategy
5. record and report,
6. monitor and review, and
7. communication and consultation.

3.1 Establish the Scope and Context

ERM principles and practices can be applied at a strategic, operational, program or project level within HOPA. It is essential to have clarity with respect to the scope of the decision, activity or process under consideration. The assessment of risk is undertaken relative to a specific objective or desired end state and requires a well-developed understanding of both the internal and external context impacting the risk being assessed.

The following questions help to articulate and establish greater clarity for scope and context and should be considered during the process:

a. What process, project, operation, or governance activity is under review?
b. Are there related activities, projects or processes that should be taken into consideration?
c. Who should be involved in the risk assessment process? Keep in mind that ERM must be embedded at all levels of governance and operations.
d. Who should be consulted? Consider both the integral nature of ERM activities and the need to develop context. Communication and consultation with stakeholders are important throughout the process to promote awareness and understanding of risk and to ensure that decision-making is based on the best available information.
e. Is the internal and external context well understood? If not, what additional information or expertise is required?
f. Is the best available information? Are all appropriate sources considered?
g. What limitations, human, cultural, financial and/or other, might impact the risk assessment process?

h. Are there other questions relevant to the scope or context under consideration?

Discussions and decisions regarding scope and context are essential components to the ERM process. The above considerations should become embedded within risk conversations, discussions and normal operations. For significant risk decision making, these details should form part of the record keeping. A form for recording the decisions is attached as Appendix A. Appendix B provides resources for determining the information and source of information on the internal and external context.

3.2 Establish the Risk Criteria

Risk criteria (commonly referred to as risk appetite) is the amount and type of risk that is acceptable to take relative to the achievement of objectives. Risk criteria is set by the Board and it may be described in a single broad policy statement or in relation to specific types of risk, such as financial or strategic. It may be qualitative, quantitative or a combination of both and should align with the mission, vision, values and strategy.

In addition to confirming scope and context, you must identify whether the risk criteria have been established for the activity under review. The risk criteria will provide the benchmark against which a risk is assessed to determine whether the level of risk is acceptable and the response strategy.

Risk tolerance is used to provide additional sensitivity to risk criteria by establishing level of variation we are willing to accept or not accept in the pursuit of specific objectives. Defined risk tolerance levels inform the decision-making process for selecting the most appropriate risk response.

3.3 Risk Assessment

Risk assessment is the process of risk identification, risk analysis and risk ranking.[5]

3.3.1 Risk Identification

The risk identification step allows HOPA to identify, and where appropriate, documents potential threats to the achievement of HOPA's objectives. It includes any material event or condition that

[5] ISO 31000:2018(E)

could affect HOPA's long-term performance or cause destruction of subscriber value. Risk categorizes are often used to assist with the organization of risks. The categories are used to segregate similar risks into manageable groupings. The use of categories also encourages a more comprehensive view of risks across the system. Some risks fit nicely in to one category while many overlap multiple categories. HOPA has defined six risk categories: strategic, financial, organizational, legal/compliance, operational, and external.

Strategic Risk	Any risk associated with the formulation or execution of a strategy designed to achieve specific objectives. Sources of risk include; flawed plan or execution and board oversight.
Financial Risk	Exposure related to financial management and performance, including; equity management, working surplus, risk margin, premium stability, forecasting, and investment performance.
Organizational Risk	Exposures related to ineffective management, insufficiency of competencies and deployment of staff, and failure to attract, motivate, train, retain and deploy talent including cultural considerations.
Operational Risk	Risks associated with the day-to-day running of HOPA, including; leadership quality and depth, performance, retention and availability and cultural alignment.
Legal & Compliance Risk	Compliance with applicable laws, regulations, reporting requirements and exchange agreement.
External Risk	Exposures related to potential events or occurrences beyond HOPA's direct control.

The inclusion of "Reputation" as a specific risk category is often debated within ERM resources. HOPA has not identified this as a separate category as we acknowledge that a negative impact on HOPA's reputation is a potential outcome of an adverse event under any of the risk categories.[6] The impact of damage to reputation is a compounding factor that should be addressed in relation to all identified risks. (See page 11 for additional discussion.) The appropriate response strategy may differ from the underlying risk; the impact of reputation loss is often felt for longer periods of time and it may require separate accountability and reporting requirements.

[6] ICD

All identified risks should be listed on the Risk Identification List - Appendix C. The purpose of the Risk Identification List is to provide an overview of all potential threats. This is simply a list. It does not include an analysis of the risk in terms of severity and likelihood.

3.3.2 Risk Analysis

Once the risks have been entered on the Risk Identification List, they are then assessed to determine the risk score. This process includes assessing each risk in terms of severity (i.e. what would be the consequences of the risk materializing) and then in terms of likelihood (I.e. how likely is it that the risk will occur).

Severity is rated on a scale of 1 – 5 based on the perceived impact, if the risk occurred, on organizational performance or subscriber value. Severity should be considered first without regard to likelihood to avoid inadequate consideration of a risk that while severe is improbable.[7] The impact on subscriber value or organizational performance may be qualitative, quantitative, or a combination of both.

The table below outlines the criteria for scoring severity:

1 Low	No material impact on organizational performance or Subscriber value and can be managed within current resources.
2 Moderate	Could affect organizational performance or Subscriber value and can be managed with current or additional operating resources.
3 High	Results in some degradation in organizational performance or Subscriber value and is likely to require an unanticipated use of capital.
4 Very High	Results in a significant degradation in organizational performance or Subscriber value and is likely to require an immediate unanticipated increase in capital (reserve or surplus).
5 Catastrophic	Threatens HOPA's long-term viability.

Prior to finalizing the final risk score, there are 4 compounding factors that should be considered: damage to reputation, shared risk, risk clock-speed and interconnectivity of unrelated risks.

1) Damage to reputation can result from any of the risk categories. It can have severe and long-lasting impact, potentially longer lasting than the underlying risk. It also may require a different treatment to mitigate or resolve. Damage to the HOPA's reputation should be

specifically considered when assessing the severity and likelihood rating of each identified risk.

2) In some circumstances the ownership of the risk may be shared and the ability to accurately assess the risk in terms of severity and likelihood and to effectively implement and monitor the risk response may be impacted. Also, the risk response strategy may be different for shared risks.

3) Risk clock-speed is the time that it will take to respond to an event and the additional risk that arises between the recognition of the event and the response. [8] For example, the time required to gather the information necessary to understand and manage a risk. It raises the question, can HOPA implement the response strategy and still function effectively? Also, what additional resources would be required? The answer to these questions may impact both the severity and likelihood ratings.

4) Consideration should be given to the interconnectivity of risk. This is the effect of unrelated occurrences that arise at the same time. For example, the effect of a single event combined with several higher risk conditions that have been present for a considerable period of time. Consider whether there are conditions present that may result in a compounding effect and whether the severity and/or likelihood ratings should be adjusted.

Once the applicable compounding factors have been considered, the severity rating should be adjusted.

The next step is to assess the risk in terms of likelihood that the event or condition will materialize by estimating the frequency of the risk occurring using the scale below.

Considerations that may assist in applying judgement to the assessment of likelihood are past history, knowledge of the industry/sector, and internal and external environment.

1	Rare	No prediction confidence
2	Unlikely	There is a remote chance that the risk will occur.
3	Possible	The risk may occur, or risk is emerging with a timeline that is longer and maybe up to 10 years.
4	Likely	There is a probability that the risk will occur, and the timeframe is likely to be within 5 years.
5	Almost Certain	Expected to occur and with a close timeframe of the next 2 years.

Assign the likelihood rating on the Risk Register Appendix D. Consider whether any of the compounding factors (page 11) increase the likelihood and adjust the rating accordingly.

3.3.3 Risk Score

Risk score is the product of risk severity rating times the risk likelihood rating. Each risk should be ranked and then be added to the Risk Register, Appendix D. Consideration may be given to limiting the number of risks entered into the Risk Register to ensure that those risks with the highest rank are prioritized for the purpose of implementing an appropriate and timely response strategy.

The risks are then plotted on the Risk Matrix – Appendix E.

RISK MATRIX						
SEVERITY	5 Catastrophic	5	10	15	20	25
	4 Very High	4	8	12	16	20
	3 High	3	6	9	12	15
	2 Moderate	2	4	6	8	10
	1 Low	1	2	3	4	5
Likelihood		1 Rare	2 Unlikely	3 Possible	4 Likely	5 Almost Certain

3.3.4 Risk Response

The purpose of identifying the risk response is to select and implement options for addressing the identified risk. Risk response involves an iterative process of:

- formulating and selecting risk response options
- planning and implementing risk response
- assessing the effectiveness of that response
- deciding whether the remaining risk is acceptable, and if not acceptable
- taking additional risk response measures. [9]

The selection of risk response options involves balancing the potential benefits of introducing further risk response (controls) against the associated cost, effort or disadvantages.[10]

Risk response options are not necessarily mutually exclusive or appropriate in all circumstances. The appropriate risk response strategy should be determined while considering whether a risk introduces a potential negative impact or may give rise to an opportunity. Strategies that can be

[9] ISO
[10] ISO 31000

applied to negative risks (threats) and positive risks (opportunities) are detailed in the table below. [11]

Strategies for Negative Risks / Threats The purpose of a negative risk response strategy is to either avoid or minimize the impact of a negative risk.		**Strategies for Positive Risks / Opportunities** The objective of positive risk response strategies is to increase the chance of the risk occurring and realize it if it occurs.	
Accept	In the accept risk response strategy, you take no action except acknowledge it. This strategy is used for non-critical risks or if the effort involved does not outweigh the benefit. This risk response strategy can be active or passive. In active acceptance you keep a contingency reserve to manage it, and in passive acceptance you do nothing except note it down in the risk register.	**Accept**	The accept risk response strategy can be used with both types of risks. Here you take no action, and if a positive risk occurs you will benefit.
Transfer	The transfer risk response strategy is used when you cannot manage the risk on your own. For example, you are lacking resources, skills, or time. Here the management of the risk is transferred to a third party. If the risk occurs, it will be their responsibility to manage it.	**Share**	In the share risk response strategy, you will join or invite someone else to realize the opportunity together as you are not able to realize the opportunity on your own.
Mitigate	In the mitigate risk response strategy, you try to minimize the probability of the risk occurring or its impact.	**Enhance**	In this risk response strategy, you increase the chance of the risk happening so if the risk occurs you can realize it. The enhance risk response strategy is the opposite of the mitigate risk response strategy where you reduce the probability of the risk happening or its impact
Avoid	This is the best strategy to manage a risk if it is an available option. Here, you avoid the risk by changing the scope, planning or schedule.	**Exploit**	In the exploit risk response strategy, you make sure that the risk is realized. This response strategy is the opposite of the avoid risk response strategy where you ensure that the risk do not occur.

Once the risk response options have been chosen, a risk response plan should be developed and documented using the Risk Response Worksheet (Appendix F). The worksheet includes documentation of the;

- risk statement
- risk score
- frequency of monitoring

[11] Risk Response Strategies in Project Management, Fahad Usmani PM Sprout March 29, 2018

- risk response strategies
- tactics associated with the risk response plan
- responsibility(s) for implementing the plan

In some circumstances residual risk will remain even after risk treatment. When there is residual risk, the risk should continue to be monitored and reviewed periodically to assess whether the residual risk requires further action. If further action is required, the residual risk response should be developed by implementing a separate risk response plan as outlined above.

3.3.5 Record and Report

The severity of the risk along with the risk appetite and tolerance of the organization should guide how often a risk should be monitored. Low to moderate risk should be reviewed annually, whereas risk rated high and above require review quarterly. Monthly review of a risk may be scheduled as needed – particularly when the risk is quickly evolving, or the Board's tolerance for the risk is greatly exceeded. All worksheets should be reviewed by the Risk Management committee twice per year.

The report from the Risk Management committee to the Board should occur twice per year and include:

- A review of the current Risk Register
- Risk Response Worksheets for risks scored high and above, and others at the request of the Board.
- Identification of risks not currently on the risk register, including their risk assessment and recommended risk response plan

3.4 Communication and Consultation

Communication of risk and consultation with stakeholders are integral to the entire ERM process. Communication seeks to promote awareness and understanding of risk, whereas consultation involves obtaining feedback and information to support decision-making. Close coordination between the two should facilitate factual, timely, relevant, accurate and understandable exchange of information, taking into account the confidentiality and integrity of information as well as the privacy rights of individuals.

4 Governance

Central to the Framework is the commitment to embedding ERM into HOPA's governance, management and operations. ERM is a core Board responsibility that includes:

- Approval, and regular review of the Framework to ensure that it remains appropriate to HOPA's size and complexity and the maturity of the ERM program.
- Leadership by communicating HOPA's commitment to ERM internally and externally, and by ensuring that enterprise risk management is an integral part of Board governance and strategic decision making.

The Board will appoint a Risk Management Committee with lead responsibility for ERM, including:

- an advisory role to assist the Board and CEO with the design, implementation, and evaluation and improvement of the ERM Program,
- ensuring the ongoing review (at least once every 2 years) of the Framework and a process for recommending changes to support the continued development of ERM;
- assisting with the ERM process of identifying and managing risk,
- reporting to the Board on risk assessment and risk response plans, and
- facilitating meetings of the Risk Management Committee with other committees and management to ensure the effective and efficient implementation of ERM practices and processes.

The Board will delegate to senior leadership operational responsibility for ERM, including accountability and authority to manage risk. Board senior leadership recruitment will identify enterprise risk management expertise as a key competency.

The Board will consider the financial resource needs of the ERM program at least annually with the annual operating budget approval process.

The Board will review HOPA's approved Enterprise Risk Management Policy (Appendix G) at least every 2 years or as determined to be appropriate by the Board.

5 Appendices

5.1 Appendix A - Scope and Context Worksheet

Scope and Context Worksheet				
Strategy, Process or Activity				
Participants				
Internal Context & Information				
External Context & Information				
Stakeholder Consultation				
Limitations				
Risk Criteria				
Risk Identification				
1.	Risk Category		Objective Impacted	
Description		Severity Rating:		
Reputation Risk Risk Clock Speed Interconnectivity Shared		Adjusted Severity Rating:		
Likelihood rating:			Risk Rank:	
Enter into Risk Identification List				

5.2 Appendix B - Context

HOPA is an insurance reciprocal exchange established by subscribing members in 1992 to provide stable, cost-effective insurance and risk management services. As a reciprocal exchange insurer, HOPA is an unincorporated association created by the exchange of contracts of mutual indemnity or inter-insurance between subscribers who are each contractually liable for the losses of the program. HOPA is licensed and regulated by the office of the Superintendent of Insurance (NS).

HOPA's internal context includes:	Internal Sources of Information includes:
• Reciprocal sector: legal and regulatory environment • Program structure, membership and funding • Subscriber base: perception, expectations, needs and values • Internal stakeholders: perceptions, expectations, needs and values • Culture: mission, vision, values and principles • Strategy and objectives • Competitive differential, strengths and weaknesses • Resources: capital, time, people, processes, systems and technologies • Self-assessment	• Mission, Vision, Values • Exchange Agreement - HOPA reciprocal structure, responsibilities and authority • Strategic Plan • Environmental scan • Actuarial Review and Funding Recommendation • Audit Report and audited FS • Business Plan • Subscriber Survey Feedback • Equity Management Policy • Subscriber Equity Accounts • Investment Policy • Investment Manager Reports • Scenario planning
HOPA's external context includes:	External Sources of Information
• External stakeholders, including their perceptions, expectations, and needs • Reciprocal industry key drivers & trends • Commercial insurance industry drivers & trends • Competitors: differential advantage • Economic factors including investment outlook • Political environment	• Health care sector • Reciprocal sector • Commercial Insurance Sector • Broker sector • Financial sector • SOI and Insurance Act (NS) • IFRS Guidelines • Independent Consultants, Actuarial, Audit, Broker, claim counsel, corporate counsel

5.3 Appendix C - Risk Identification List

	Objective	Risk Category	Risk Description	Date
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				

5.4 Appendix D - Risk Register

Risk Register								
	Risk Category	**Risk**	**S**	**L**	**Risk Tolerance**	**Action**	**Accountability**	**Reporting Frequency**
			Rank					
1.								
2.								
3.								
4.								
5.								
6.								
7.								
8.								
9.								
10.								

5.5 Appendix E – Risk Matrix

RISK MATRIX						
SEVERITY	5 Catastrophic	5	10	15	20	25
	4 Very High	4	8	12	16	20
	3 High	3	6	9	12	15
	2 Moderate	2	4	6	8	10
	1 Low	1	2	3	4	5
Likelihood		1 Rare	2 Unlikely	3 Possible	4 Likely	5 Almost Certain

SEVERITY	
Low	No material impact on organizational performance or Subscriber value and can be managed within current resources.
Moderate	Could affect organizational performance or Subscriber value and can be managed with current or additional operating resources.
High	Results in some degradation in organizational performance or Subscriber value and is likely to require an unanticipated use of capital.
Very High	Results in a significant degradation in organizational performance or Subscriber value and is likely to require an immediate unanticipated increase in capital (reserve or surplus).
Catastrophic	Threatens the long-term viability of the Association.

LIKELIHOOD	
Rare	No prediction confidence
Unlikely	There is a remote chance that the risk will occur.
Possible	The risk may occur, or risk is emerging with a timeline that is longer and maybe up to 10 years.
Likely	There is a high probability that the risk will occur, and the timeframe is likely to be within 5 years.
Almost Certain	Expected to occur and with a close timeframe of the next 2 years.

Risk Level	Risk Score	Review Frequency
Low	1 – 4	Annually
Moderate	5 – 9	Annually
High	10 – 15	Quarterly
Very High	16 – 25	Quarterly, or as required.

5.6 Appendix F – Risk Response Worksheet

HOPA DRAFT Risk Mitigation Worksheet

Risk Analysis: (Risk) Date:					
Risk Statement:				RISK MATRIX	
				SEVERITY 5	
				4	
				3	
				2	
Risk Tolerance:				1	
				RISK SCORE:	1 2 3 4 5 LIKELIHOOD

		Opportunity			Review Frequency
Accept – Used for non-critical risks or if the effort involved does not outweigh the benefit. Can be active or passive. Active – Keep a contingency reserve to manage it. Passive – take no action except to note it in the risk register	☐	**Accept** - Take no action, and if a positive risk occurs you will benefit.	☐	1-4	Annually
Transfer – Cannot manage the risk on your own. Lacking resources, skills, time. Management of risk is transferred to a third party	☐	**Share** - Join or invite someone else to realize the opportunity together as you are not able to realize the opportunity on your own.	☐	5-9	Annually
Mitigate – Minimize the probability of the risk occurring or its impact.	☐	**Enhance** - Increase the chance of the risk happening so if the risk occurs you can realize it.	☐	10-15	Quarterly
Avoid – Best strategy if available. Avoid the risk by changing the scope, planning or schedule.	☐	**Exploit** - Make sure that the risk is realized.	☐	16-25	Quarterly/as needed
Residual Risk:		Target Risk Level:		Target Date:	

Risk Response Plan			
Objective:	Lead	Reports to	Target Date Completion
Description:			

5.7 Appendix G - Enterprise Risk Management Policy

Health Organizations Protective Association
POLICY & PROCEDURE

Subject/Title:	**ENTERPRISE RISK MANAGEMENT (ERM)**	Approval Date: Date Revised:
Approving Authority:	Board of Directors	**Reference Number:**
Classification:	Governance	Last Review: Next Review:

PURPOSE

The Health Organizations Protective Association (HOPA) is committed to implementing and maintaining an effective enterprise risk management (ERM) program to support the creation and protection of value and the achievement of HOPA's objectives. To this end, the Board has approved an ERM Framework to ensure a reliable and consistent approach to the recognition of and response to potential sources of risk.

POLICY

The Board of Directors is responsible to:

1. Approve an ERM Framework
2. Establish the amount and type of risk (i.e., tolerance) that may or may not be taken relative to the achievement of objectives
3. Review the ERM Framework once every two years to confirm that it remains appropriate
4. Implement internal and external stakeholder communication and consultation plans
5. Ensure the required ERM competencies to apply the ERM Framework are included in board and committee composition and senior leadership team
6. Incorporate ERM training in the director orientation and other board development as required
7. Ensure the board annual agenda planning includes the ERM
8. Ensure committee terms of reference include ERM responsibilities
9. Assign authority, responsibility, accountability for the Board, Committees and CEO
10. Allocate the financial resources required to support the ERM Framework activities.