Enterprise Risk Management

Policy Owners:	Fire Life Safety & Risk Management
Approval:	Board of Directors
First Approved:	December 6, 2018
Effective Date:	December 6, 2018

Policy Statement

Toronto Community Housing Corporation (TCHC) will take measures to ensure appropriate oversight of the enterprise-wide risk profile. TCHC will identify all priority risk exposures and implement appropriate risk treatments to mitigate the exposures to within the established risk appetite. This will support the advancement of a culture that shapes how risk decisions are made and which enhances value to TCHC's shareholder, tenants and stakeholders.

Using an Enterprise Risk Management (ERM) framework, TCHC will systematically identify, assess, and monitor potential, actual and emerging enterprise risk exposures. Identified risk exposures and associated treatment and mitigation plans will inform enterprise-wide planning and risk-informed decision making. As well, identified risk exposures will be integrated as key inputs to assist in prioritization into the corporation's four-year strategic plan, internal audit plan, and divisional business plans.

Scope

The ERM policy outlines TCHC's philosophy and approach to the management of risk exposures across the corporation. The policy highlights the fundamental structure, processes, and elements contained within the ERM framework, which support the achievement of TCHC's strategic goals and objectives.

In addition, this policy outlines the key roles and responsibilities of the ERM Committee. The committee provides corporate oversight on the advancement of the ERM framework to ensure that TCHC identifies all enterprise risk exposures and implements the appropriate risk treatment plans.

Definitions

Risk Exposure: The negative or positive deviation from the expected outcome.

Enterprise Risk Management: The structure and process effected by an organization's board of directors and management to enable the identification, assessment, evaluation and monitoring of potential, actual, and emerging risk exposures.

Risk Appetite: The amount and type of risk exposure that an organization is willing to accept to achieve its strategic objectives or desired outcomes. Often, this is formalized and conveyed to the organization via risk appetite statements.

Policy Details

The TCHC ERM program will be administered through the following three components: governance, framework, and policies and procedures. Together, the components provide the foundational structure and processes affecting the organization's ERM activities.

Governance

The ERM governance shall ensure that the appropriate structure and processes are in place to enable appropriate oversight and monitoring of the enterprise risk profile and, where applicable, provide the appropriate escalation and disclosure mechanisms for material risk exposures. As well, the governance will support consistency of ERM activities across the organization, establish clear roles and determine how risk exposures are addressed. The key elements and enablers of the ERM governance are:

a. **Board of Directors:** The Board of Directors shall have accountability to oversee the ERM program, including the governance and advancement of the ERM framework**.** This oversight includes establishing the appropriate infrastructure supported by relevant policies and procedures, and enabling enterprise-wide risk identification, monitoring and evaluation of risks against the established risk appetite.

b. **ERM Committee:** The committee shall have accountability to provide corporate governance and oversight on the advancement of the ERM framework at TCHC. This would include the identification, monitoring, and evaluation of risks against the established risk appetite, as well as enhancing and supporting ERM capacity and engagement.

c. **Corporate ERM:** The Corporate ERM department shall have accountability for the strategic and operational administration of the ERM and its corresponding framework. This includes providing support for the enterprise-wide risk identification, monitoring and evaluation process, and to each of the functional areas to enhance capacity and engagement.

Framework

The ERM framework shall ensure that the appropriate methodologies and tools are in place to support TCHC to identify, assess and monitor potential, actual or emerging risk exposures. As well, the framework contains and applies elements of industry best-practices (e.g., COSO, ISO 31000, Value-Based) suitable to the size and complexity of the TCHC ERM framework. The key elements and enablers of the ERM framework are:

Risk Register: The risk register shall be the centralized and standardized electronic repository for identified risk exposures through the ERM framework. The risk register will document essential risk information, including but not limited to the risk statement, risk likelihood, risk impact, risk rank score, risk appetite, and risk action plan. The Corporate ERM department shall be the system administrator and information custodian of all information contained in the risk register.

Risk Domains: The risk domains provide a standardized methodology/approach to classify risk exposures. This will further support standardization and consistency in how risk exposures are categorized and communicated across the organization. The risk domains consist of the following three main risk categories and 10 risk-subcategories (see Appendix A):

1. **Business Risks**

Risk exposures that impact the delivery of services to our tenants and stakeholders. It includes the following risk-subcategories:

- Business Operations
- Reputation and Public Image
- Governance

2. **Resources Risks**

Risk exposures that relate to the resource used by the organization to deliver our services. It includes the following risk-subcategories:

- Human Resources
- Financial

- Information Systems
- Physical Assets

3. Compliance Risks

Risk exposures that relate to the ability to comply with regulatory requirements. It includes the following risk-subcategories:

- Environment, Health and Safety
- Legal, Regulatory and Standards
- Policies and Procedures

Risk Criteria

The risk criteria provide a standardized methodology/approach and levels to support the evaluation and prioritization of the significance of risk exposures across the organization. They are also a key input into the enterprise risk register. The key factors of the risk criteria are (see Appendix B):

- Risk Likelihood: The possibility that a risk incident or exposure will occur;
- Risk Impact: The extent to which a risk event might affect TCHC; and
- Risk Score: The overall score reflective of risk likelihood and impact.

Risk Management Cycle

The risk management cycle is an integral part of the overall management of risk exposures across the organization. The key steps of the cycle are the identification, assessment, evaluation, treatment and monitoring of risks.

1. Identification

The risk identification step involves identifying potential, actual or emerging risk exposures for the organization. This step shall take into consideration the risk causes and impacts, as well the risk treatments implemented to manage the risks within the organization’s established risk exposure.

2. Assessment

The risk assessment step involves further evaluation and prioritization of the risk exposures by analyzing each of the identified risks based on both risk likelihood and risk impact. The risk likelihood and risk impact will inform the total risk score. The results of the risk assessment shall be a key input into the corporate risk profile.

3. Evaluation

The risk evaluation step involves risk-informed decision making, as each identified risk is evaluated according to its total risk score. This step includes an evaluation of the corporate risk profile and discussion of the priority risk exposures for the organization. Typically, the prioritized risk exposures for a calendar year shall be no more than 10 risks. Lastly, a risk lead shall be assigned to be the appointed owner of managing a priority risk, including the development and implementation of a risk treatment plan.

4. Treatment

The risk treatment step involves the development and implementation of a plan that would include a set of risk controls that would be aimed to modify the risk likelihood, risk impact or both to within the established risk appetite. The risk treatment plan shall use a combination of the following risk controls:

- Avoidance: The elimination of threats, causes or hazards that would result in an impact on an organization.
- Reduction: The reduction of damages or losses resulting from a risk exposure/incident.
- Transfer: The contractual shifting of a risk exposure/incident to a third-party entity.
- Acceptance: The acknowledgement and acceptance of any damages and/losses that could result from a risk exposure/incident.

Related Policies and Procedures

The ERM policies and procedures shall formally document and communicate the key elements of the ERM governance at TCHC. Through the policies and procedures, TCHC will outline the organization's philosophy and approach to the management of risk exposures across the organization. The key documents within the ERM policy and procedures are:

ERM Policy: This policy shall outline TCHC's philosophy and approach to the management of risk exposures across the organization. In doing so, it will highlight the fundamental structure, processes, and elements contained within the ERM framework, which is in support to the achievement of our strategic goals and objectives.

Risk Appetite Policy: This policy shall outline TCHC's risk appetite across the organization specific to each of the established risk domains. In doing so, it will highlight risk appetite statements that convey the amount of risk exposure that the organization is willing to seek or accept in pursuit of its strategic goals and objectives. As well, the policy will outline risk preferences that convey the types of risks the organization is willing to take to support its overall advancement.

Compliance and Monitoring

The Corporate ERM department will monitor compliance to the ERM Policy. The risk monitoring step shall involve active oversight over the corporate risk profile, which includes the priority risk exposure factors and treatment plans. The ERMC shall be immediately notified by the Corporate ERM department or Risk Leads of any priority risk exposures that may have shifted risk factors and of the treatment plan that would result in either a potential or actual breach of the established risk appetite.

Related Policies and Procedures

- Risk Appetite Policy

Commencement and Review

Revision	Date	Description of changes	Approval
First approval:	December 6 2018		Board of Directors
[Revision #]			
Last review:			

Next Scheduled Review Date: December 6, 2020

Appendix A: Risk Domains

Business Risks Risks that impact the delivery of services to our tenants and stakeholders	**Resources Risks** Risks that relate to the resource used by the organization to deliver our services	**Compliance Risks** Risks that relate to the ability to comply with regulatory requirements
Business Operations Service Delivery Operational Partnerships Cleaning & Maintenance	**Human Resources** Labour Relations Talent Management Culture	**Environment, Health & Safety** Environmental Management Occupational Health & Safety Life & Safety Systems
Reputation & Public Image Public Image Media Exposure Government Relations	**Financial** Operational Funding Working Capital	**Legal, Regulatory & Standards** Legislation Compliance Regulatory Standards
Governance Governance	**Information Systems.** Infrastructure Data Integrity, Security & Privacy Business Continuity	**Policies & Procedures** Policy Development & Compliance Policy Education
	Physical Assets Buildings Equipment	

Appendix B: Risk Criteria

Likelihood: The possibility that a given risk incident/exposure will occur.

Rating	Description	Definition
1	Very Low	Very unlikely to occur, but not impossible
2	Low	Low likelihood to occur
3	Moderate	Possible that it may or may not occur
4	High	High likelihood to occur
5	Very High	Very high likelihood to occur

Impact: The extent to which a risk event might affect TCHC

Rating	Description	Definition
1	Very Low	Minimal impact on operations
		High enterprise level/process capabilities to address risks
2		Contingency and crisis management plans in place
		High operational/process efficiency
3	Moderate	Moderate impact on operations
		Medium enterprise level/process level capabilities to address risks
4		Most contingency and crisis management plans in place
		Medium operational/process efficiency
5	Very High	Significant or major impact on operations
		Lack of or low enterprise level/process level capabilities to address risks
		Lack of or low contingency or crisis management plans in place
		Lack of or low operational/process efficiency