

WSIB OVERSIGHT POLICY

TITLE: Corporate Risk Management Policy

OWNER: Corporate Risk Management Services

Table of contents

- Overview 3
- Purpose 3
- Application and scope 3
- Policy statement 3
- Definitions 4
- Requirements 5
 - 1. Guiding principles 5
 - 2. Risk appetite and risk tolerance 7
 - 3. ERM Program 8
 - 4. Governance: roles and responsibilities 8
- Policy maintenance 15
- Related documents 15
- Effective date 15

Overview

The Corporate Risk Management Policy (“policy”) sets out objectives, scope and approach, guiding principles, risk appetite statements, and risk governance for the Workplace Safety and Insurance Board (“WSIB”) to ensure consistent and effective management of risk.

The WSIB has adopted an enterprise-wide approach to risk management based on the ISO 31000¹ and COSO² framework standards (The ERM framework). The ERM framework is managed by the ERM Branch within the Corporate Risk Management Services Division, across the WSIB.

Purpose

The purpose of this policy is to set out expectations for risk management within the WSIB. This policy outlines the role of the Board of Directors (the “BOD”) and its respective committees in risk oversight, as well as what is expected of all WSIB management, employees, and the Corporate Risk Management Services Division in the performance of risk management and risk oversight.

Application and scope

The scope of the policy is enterprise-wide and is applicable to the BOD and its committees, management, and across all business areas and levels of the WSIB.

This policy serves as an umbrella policy for internal (corporate and functional) policies that pertain to individual risks that exist at the WSIB.

Policy statement

The WSIB is committed to managing risks related to the achievement of the organization’s strategic objectives as identified in its multi-year strategic plan.

Risks shall be managed in accordance within the BOD-approved ERM Strategy, and in a manner that is integrated in its approach, balances risks and rewards, supports risk-based decision-making, facilitates improved corporate and risk governance, and is consistent with the

¹ International Organization for Standardization’s risk management standard, ISO 31000

² Integrated Framework for Enterprise Risk Management, developed by the Committee of Sponsoring Organizations of the Treadway Commission.

stated WSIB's values. Furthermore, it recognizes that certain risks must be taken in pursuit of the objectives of the business.

Definitions

For the purposes of this policy:

Enterprise risk management: a process, applied by our organization in a strategic setting, which enables management to (i) identify potential risk events that may affect the WSIB; and (ii) provides a framework to manage risk within the organization's risk appetite and risk tolerance levels in order to provide reasonable assurance that, in the pursuit of the organization's objectives, an appropriate level of risk is accepted. This includes culture, capabilities, practices, integrated with strategy-setting and its performance.³

Enterprise risk management framework: a set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization. The Framework operationalizes the Corporate Risk Management Policy.⁴

Event: occurrence or change of a particular set of circumstances, from sources internal or external to the WSIB, that could affect (i.e., positively or negatively) the implementation of strategy or achievement of objectives by being a source of risk.⁵

Opportunity: An action or potential action that creates or alters goals or approaches for that can positively affect the achievement of objectives.⁶

Residual risk: Residual risk is the risk remaining after management's response to the risk.⁷

Risk: the possibility that an event will occur and adversely affect the achievement of the WSIB's strategic and operational objectives.⁸

³ Adapted from the Committee of Sponsoring Organizations of the Treadway Commission's (COSO) ERM 2017 Definition

⁴ Adapted from International Standard – Risk Management Practices and Principles (ISO 31000: 2018)

⁵ Ibid (see footnote 2)

⁶ Ibid (see footnote 2)

⁷ Adapted from the Committee of Sponsoring Organizations of the Treadway Commission's (COSO) ERM 2004 Definition

⁸ Ibid (see footnote 3)

Risk appetite: The types and amount of risk, on a broad level, the WSIB is willing to accept in pursuit of value.⁹

Risk owner: A person or persons that have been given the authority to manage a particular risk and are accountable for doing so.¹⁰ Risk owners for the Significant Enterprise Risks are Chief Officers.

Risk tolerance: As set by management, the level of variation the WSIB is willing to accept relative to the achievement of objectives as a result of specific risks; it is the **maximum** and **minimum** acceptable variation that are tied to the overall Risk Appetite.¹¹

Significant enterprise risk: inherent in our business and operations, these risks alone or in combination with other interrelated risks, can have a significant adverse impact on the organizations' reputation, financial, and/or operational performance, or ability to service our customers. These risks are identified by management and approved annually, within ERM Strategy, which is by the Board of Directors.

Significant enterprise decisions: include oversight, corporate or operational level decisions that:

- set and/or change the WSIB's strategy and priorities or the required resources; or
- carry Significant Enterprise Risks, but are within the WSIB's risk appetite and tolerance levels; or
- have an impact on more than one cluster or require consultation with stakeholders; or
- have an urgency, but where the consequences are not yet fully understood; or
- fall outside of the WSIB's risk appetite or could adversely impacts WSIB's reputation.

Requirements

1. Guiding principles

ERM at the WSIB is guided by the following key principles:

- **Risk management is part of decision making** – the WSIB shall make decisions that involve a level of risk that is in line with its BOD-approved risk appetite and management's approved risk tolerances. Effectively managing risk and allocating resources through optimized risk/reward decision making is essential for the

⁹ Ibid (see footnote 3)

¹⁰ Ibid (see footnote 3)

¹¹ Ibid(see footnote 2)

organization to achieve its strategic objectives and financial aspirations, meet its legislative obligations, and protect its reputation.

- **Decisions shall be supported by risk analysis**, commensurate with the significance of the decision, including an assessment of the alignment with WSIB's risk appetite. An independent risk assessment undertaken by the Corporate Risk Management division is advisable for Significant Enterprise Decisions.
- **Risk management is an integral part of all organizational processes** – Risk supported analysis and active risk management is a part of management activities and an ongoing responsibility of individuals at all levels within the organization. It must be embedded in business planning, decision making, program and project management, change management, oversight activities, reporting and day-to-day activities with the aim of ensuring risk-informed decisions and actions.
- **Risk management is systematic, structured and timely** – Risk management standards are in place to promote consistency and best practices in the managing, monitoring and reporting of risks including a risk taxonomy used by the organization in discussing risk.
- **Risk management is transparent** – The risks facing the WSIB or any function within the WSIB can only be understood, analyzed, assessed or managed by those who understand the broader context within which such risks have emerged and continue to evolve. ERM implementation will engage stakeholders and, in particular, decision makers from all levels of the organization to ensure that risk management remains relevant and up to date.
- **Risk management is dynamic, iterative and responsive to change** – Risk management continually senses and responds to change and supports decision-making. As external and internal events occur, context and knowledge change, monitoring and review of risks take place, risks emerge, change and disappear.
- **Reporting** – Risks will be identified and reported regularly and on an ad-hoc basis (as needed) to Risk Owners, Executive Committee and Committees of the Board of Directors, as appropriate.
- **Independent assurance** – The WSIB shall obtain periodic independent assurance (i.e., through internal audit and/or external audit) that ensure systems of risk management are operating efficiently and effectively.
- **Insurance is an integral part of the WSIB's risk management program** – Specific insurance solutions shall be regularly evaluated as a mechanism to transfer risks that cannot be otherwise mitigated or eliminated and that lie outside of the WSIB's risk appetite.

2. Risk appetite and risk tolerance

A certain level of risk is inherent in the business activities of the enterprise and is the amount and type of risk the WSIB is willing to accept in pursuit of value, as defined as the WSIB's strategic objectives.

WSIB's strategic framework shall be consistent with WSIB overall risk appetite with the specific risk appetite statements being reviewed annually as part of the annual review of the Corporate Risk Management Policy.

Management operationalizes the appetite statement into key risk measures and metrics within management's approved risk tolerance levels for specific risks as identified in the reporting that is provided to the BOD's Governance Committee. Circumstances where a recommended course of action or a decision falls outside the WSIB's risk appetite statements shall be brought forward to the BOD for consideration. The organization's risk appetite statements are as follows:

- The WSIB shall maintain a high level of assurance that the sufficiency ratio will not fall below 100 per cent by collecting premium revenue to ensure recovery of administrative and new claims costs, and prudently managing investments through long-term economic cycles with the dual objectives of earning a meaningful contribution to funding while minimizing premium rate volatility.
- The WSIB shall pursue a claims management approach that prioritizes high quality return to work and recovery, while striving for continuous improvements to operational efficiency and efficacy.
- The WSIB shall maintain compliance with applicable government directives, as well as legislative, regulatory and policy requirements.
- The WSIB shall make risk informed and evidence based decisions that balance the interests of the people we serve with the WSIB's mandate and core values.
- The WSIB shall invest in innovative opportunities that result in improvements aligned to our strategic objectives, including health and safety, return to work and recovery outcomes, customer service, and financial responsibility and accountability, and that drive sustainable change.
- The WSIB shall be prepared to respond to disruptions that could impact our ability to deliver core services.
- The WSIB shall prioritize the security and protection of data.
- The WSIB shall operate in alignment with its core values by promoting ethical behavior, maintaining a healthy and safe workplace, and sustaining a valued and engaged workforce.

3. ERM Program

The WSIB shall maintain and mature a comprehensive risk management program that includes the following key attributes:

- it is enterprise-wide in scope, by providing an understanding of significant and emerging enterprise risks and the potential impact on value across the WSIB;
- it is cross-functional in its perspective, in providing a consistent discipline for managing risk;
- it is designed to analyze and support high-quality decisions, to optimize risk/reward outcomes and ensure that decisions are made within the WSIB risk appetite and managed within associated tolerances for defined risk;
- it is integrated into strategic and operational activities and reporting processes;
- it establishes risk responsibility, accountability, and ownership;
- it is designed to incorporate a number of approaches for managing risk, including avoidance, mitigation, transfer and acceptance;
- it ensures that risks are responded to in a timely and disciplined manner, through informed decisions and analysis outcomes; and
- it is enabled by the ERM Framework and practices, including ongoing and proactive monitoring through key risk indicators and metrics.

4. Governance: roles and responsibilities

The Board of Directors and senior management collectively have responsibility and accountability for setting the organization's objectives, defining strategies to achieve those objectives, and establishing governance structures and processes to best manage the risks in accomplishing those objectives.

While risk management is a responsibility of all staff at the WSIB, fundamental to effective risk management is a Board and senior management team with appropriate competencies and skills to properly oversee and manage the WSIB's risks. The following section outlines the responsibilities for risk management at the WSIB.

4.1 The Board of Directors (Board or BOD) is responsible for:

- taking steps to ensure that it has a proactive and dynamic approach that results in effective and proactive oversight of risk management;
- overseeing management's implementation of a comprehensive corporate risk management program to ensure the delivery of programs and services, and the achievement of strategic objectives, in alignment with the enterprise risk appetite and the WSIB's legislative mandate;
- approving, and monitoring, and evaluating Significant Enterprise Risks and WSIB's risk appetite to support the achievement of the organization's strategic objectives and its legislative mandate;
- holding management accountable for developing a strategy that correlates with the risk appetite of the WSIB;

- delegating specific risk oversight responsibilities to appropriate committees, in terms of reference/committee charters, to strengthen the BOD capacity in overseeing risk; and ensuring that its members have sufficient skills in strategy and risk oversight.

4.2 Governance Committee of the Board is responsible for:

As delegated by the Board, the Governance Committee is responsible for:

- overseeing the Enterprise Risk Management Strategy and Significant Enterprise Risks;
- recommending annually to the BOD:
 - Changes to the Corporate Risk Management Policy;
 - Annual ERM Strategy, including risk appetite statements and programs; and
 - Annual Risk Report;
- reviewing the quarterly risk report and make recommendations to the BOD on the management of the Significant Enterprise Risks, as appropriate.

4.3 Other Board Committees are responsible for:

- overseeing Significant Enterprise Risks specific to and as articulated in their mandates.

4.4 The President and Chief Executive Officer (CEO) is accountable for:

- providing the overall leadership, vision and direction for enterprise risk management at WSIB and promote the maintenance of a culture that identifies and addresses risks as ongoing part of business processes;
- assuming the overall responsibility and ownership for risk management with support from senior management;
- advising on matters related to reporting on risk management matters to the Board, including proposed changes to the risk appetite or any proposed improvements in the ERM Framework; and
- determining, with advice from the Executive Committee, the final course of action in circumstances that are escalated by the CRO that result in the WSIB operating outside of WSIB's risk appetite and risk tolerance levels and informing the Board of such circumstances.

4.5 Chief Risk Officer (CRO) is accountable for:

- overseeing the development and implementation of Corporate Risk Management services to ensure consistent comprehensive risk management practices across the WSIB;

- fostering a culture of risk management and risk awareness; providing guidance, training and expertise in support of this policy;
- monitoring the risk exposure and risk management activities of the WSIB;
- identifying circumstances that may result in the WSIB operating outside of risk appetite and risk tolerance levels and escalating such instances to the Executive Committee, the President and CEO, Governance Committee and the Board of Directors;
- ensuring the adequacy and effectiveness of risk management functions to support the management of risks at the WSIB;
- overseeing the development and maintenance of risk management program as well as processes and tools for identifying, assessing, managing, monitoring, and reporting on risks on an enterprise-wide level;
- providing timely and consistent flow of risk information to the Executive Committee, the President and CEO, Governance Committee and the Board;
- ensuring sufficient risk based analysis of Significant Enterprise Decisions, including all decisions requiring Board of Directors approval;
- ensuring the effective identification and management of WSIB's Significant Enterprise Risk and emerging risks; and
- providing an annual ERM Report to the Board.

4.6 ERM Branch is responsible for:

- instilling a risk intelligent culture, where employees at every level of the organization consider and manage risk as an intrinsic part of their jobs to support risk informed decisions;
- supporting the CRO with the development and implementation of the ERM Framework to fulfil the objectives and principles outlined in this policy;
- ensuring continuous improvement, implementation and operation of the WSIB's ERM framework and program, including the provision of expert advice, consultation and strategic direction to the WSIB senior management and make recommendations for improvements to the WSIB overall risk framework;
- supporting the WSIB's annual operational business planning exercise to facilitate the alignment of cluster business plans to risk mitigation commitment related to enterprise risks and support business area identification of risks related to their business activities and initiatives;
- identifying, monitoring, assessing, and reporting on Significant Enterprise Risks and emerging risks that compromise the achievement of the WSIB's strategic objectives or

expose the WSIB's business operations, including mitigating and monitoring in cooperation with senior management and their delegates;

- reporting, quarterly, on the Significant Enterprise Risks of the WSIB, including the respective residual risk rating and associated trends, emerging risks, a summary of material events during the reporting period, and key risk indicators and will be provided to the EC and the Governance Committee;
- supporting the proper identification, assessment and mitigation of risks in relation to the entire portfolio of projects and program related activities;
- providing a portfolio approach to supporting the WSIB's clusters and divisions by providing risk advisory services to its leadership as it plans and undertakes its day-to-day business operations as well as specific projects and initiatives;
- identifying and developing the WSIB's risk appetite by engaging the clusters in understanding their risks that reflect the organizations risk posture;
- presenting, annually, the risk appetite statements for BOD approval;
- facilitating the WSIB's ERM process (risk identification, risk assessment, risk response) and providing regular reports to management and BOD committees;
- engaging with internal stakeholders to monitor, analyze and challenge, where necessary, risk management activities and providing an independent view on WSIB's portfolio of risks as part of reporting;
- assisting Risk Owners and their teams with the development of risk tolerance levels, where appropriate;
- ensuring that appropriate escalation procedures are in place for events that could occur outside of WSIB's risk appetite and specific risk tolerance levels;
- providing guidance and support in navigating the risk management requirements established with the EPMO, including the development and implementation of project-specific Risk Management Plan and risk register, and supporting program activities;
- providing support to Finance and the WSIB's insurance broker or record on an annual basis to identify what residual enterprise or cluster-level risks may require transfer through insurance.

4.7 Enterprise Risk Analytics and Decision Support (ERADS) Branch is responsible for:

- supporting the CRO, Risk Owners and the ERM Branch in quantifying and monitoring enterprise and cluster-level risks, by developing and continuously updating key risk indicators and undertaking broader risk analysis to provide foresight and early warning with respect to changes in the profile of individual risks.

- supporting the BOD, the President and CEO and WSIB management by providing independent, risk-based analysis for Significant Enterprise Decisions.
- supporting Finance with corporate insurance purchasing decisions, by ensuring that residual enterprise risks are appropriately transferred through the WSIB's own business insurance portfolio; and
- supporting Strategic Procurement, Legal Services and first-line business units with third-party risk management through insurance, by establishing an enterprise-wide framework for identifying insurance requirements for vendor-managed services.

4.8 Legal Services Division is responsible for:

- providing advice and opinions to assist with understanding the legal implications of potential courses of action to effectively manage risk and to make fully informed decisions;
- participating in meetings and/or authoring reports as appropriate in connection with privileged matters; and
- engaging the Corporate Risk Management Services Division in matters which Legal Services believes could result in Significant Enterprise Risk or result in a Significant Enterprise Decision.

4.9 Treasury Operations Branch is responsible for:

- administering the day-to-day operations of the WSIB's corporate insurance program, including working with the WSIB's insurance broker of record as well as the ERM Branch in Risk to ensure that residual enterprise and/or cluster-level risks that lie outside of the WSIB's risk appetite and tolerance can be transferred through the WSIB's own corporate insurance portfolio.

4.10 Internal Audit and Corporate Compliance Divisions are responsible for:

Risks are monitored by the business, ERM Branch and other groups with risk oversight responsibilities (Corporate Compliance, Internal Audit) that combined, make up the organization's three lines of defense.

The Internal Audit Division, an independent function from ERM and other control and operational functions executed by management, is responsible for:

- providing independent assurance over the effective design and operation of risk management processes, methodologies and internal controls by performing audits and other engagements; and
- determining whether WSIB risk management, control and governance processes are adequate and functioning in a manner to ensure that risks are appropriately identified and managed (WSIB Internal Audit Charter, 2015).

4.11 The Corporate Compliance Division (“CC”) is responsible for:

- establishing and managing a program to ensure appropriate compliance with WSIB’s legislative, regulatory, governmental directives and other legal obligations, in accordance with the *WSIB Corporate Compliance Policy*.

4.12 Enterprise Project Management Office (EPMO) is responsible for:

- The EPMO is a centralized business function which operates at strategic level provides enterprise wide support on governance, program delivery, project portfolio management best practices, tools and standardized processes and is responsible, to engage Corporate Risk Management Services (CRMS) for the following:
- engaging CRMS to ensure that sound risk management practices are embedded within the program and project management approach that is required for all activities and initiatives on the enterprise portfolio of projects, including proper reflection of risk considerations within the project gating model including the creation and maintenance of a risk management plan and risk register; and
- ensuring an enterprise assessment of the WSIB’s ability to effectively resource, mobilize or execute program and project delivery in accordance with established timetables, budgets and the expected benefits as identified in the portfolio of Significant Enterprise Risks.

4.13 Strategy Cluster is responsible for:

- The Strategy and Analytics Cluster drives strategic change in support of the organization’s vision to be the leading workplace compensation board. As outlined in the 2017 ERM COSO Framework, ERM is to be integrated with strategy-setting to ensure a clear understanding of the existing risk profile for the organization as it pursues business objectives. As such, the Strategy and Analytics Cluster will work with the ERM Branch in the development of the WSIB’s Strategic Plan. This includes:
- Working collaboratively with the ERM Branch in the development of the WSIB’s Strategic Plan, including:
 - the development of the plan and the identification of specific priorities and objectives with consideration for the WSIB risk appetite and the established tolerance to support their achievement;
 - identification of risks associated with strategy options and the chosen path; and
 - mitigation of risks related to the plan’s execution and performance; and
- integrating CRMS in supporting the WSIB’s annual operational business planning exercise to facilitate the alignment of cluster business plans the enterprise risk profile and support business area identification of risks related to their business activities and initiatives.

4.14 Executive Committee (“EC”) is responsible for:

- reviewing and assessing, on a regular basis, identified significant enterprise and emerging risks through quarterly risk reporting;
- The Executive Committee is a management level committee comprised of Chief Officers, General Counsel and the President and CEO and is responsible, under the WSIB’s ERM framework, for the following: ensuring that risk management strategies are defined, documented and implemented;
- assisting in defining risk tolerance levels for Significant Enterprise Risks and risk appetite statements;
- reviewing, discussing and analyzing implications of circumstances that may result in the WSIB operating outside of risk appetite and risk tolerance levels that are brought to the committee by the CRO;
- ensuring that ERM is embedded in the WSIB’s strategic planning and annual business planning process;
- ensuring the risk management process is applied consistently at all levels and integrated into strategic, operational, financial activities and decision-making within their areas of responsibility;
- ensuring that significant enterprise decisions are supported by sufficient risk analysis to inform the decision making; and
- supporting the consistent application of the policy across the WSIB.

4.15 WSIB risk owners are responsible for:

- ensuring sound risk management processes, and practices are established to give effect to this policy and related individual risk management policies;
- championing risk management culture within their areas of responsibility and communicating risk management requirements to employees;
- with the guidance and support of the ERM Branch, identifying root causes of the Significant Enterprise Risks, identifying and implement relevant risk mitigation activities, and reporting on risk monitoring and management on an ongoing basis;
- participating with Corporate Risk Management Services on the annual ERM strategy, risk appetite statements, and risk tolerance levels in their areas;
- participating(along with their delegates) in dedicated risk workshops, to provide clarity on the roots causes for the Significant Enterprise Risks as well preventative and corrective mitigations to ensure the WSIB understands the potential impact such risks pose to the organization;

- ensuring that an appropriate level of resources are allocated, in alignment with established risk targets, in managing risk within their areas;
- overseeing the development of a risk register, risk tolerances and risk management activities at the various operational units; monitoring these activities and compliance with established risk tolerances and escalating any such instances where events could occur outside of risk tolerances, to the CRO;
- where there are multiple risk owners for a Risk, being responsible for coordinating and reconciling reporting on the management of their risk; and working alongside ERADS and ERM in develop key risk indicators (KRIs) to enable real-time monitoring of key data elements that will demonstrate the movement in the risk assessment and enable the WSIB to establish an appropriate risk corridor for each of the Significant Enterprise Risks.

4.16 All WSIB employees are responsible for:

- recognizing that risk management is everyone's responsibility and managing and reporting risk at the source, as appropriate to their roles, in their day to day actions; and
- continuously learning about risk management.

Policy maintenance

Corporate Risk Management Services is the owner of this policy and is responsible, for its development, implementation, annual review, update, and communication.

Related documents

- Agencies and Appointments Directive, Management Board of Cabinet, April 2018
- ISO 31000:2018 Risk Management – Principles and Guidelines
- ISO Guide 73 Risk Management – Vocabulary
- Memorandum of Understanding between the Minister of Labour and WSIB
- COSO Enterprise Risk Management – Integrated Framework, June 2017
- Guide to the Risk-Based Approach to Provincial Agency Oversight, 2018

Effective date

The Effective Date of this policy is December 13, 2018.