Computershare Trust Company of Canada
Computershare Advantage Trust of Canada
Basel III Pillar 3 Disclosures

December 31, 2025

Introduction and Scope

This document represents the Pillar 3 disclosures of the Basel III framework as required by the Office of the Superintendent of Financial Institutions (OSFI) on the general qualitative information on Computershare Canada's operational risk framework.

Computershare Trust Company of Canada ("CTCC") and Computershare Advantage Trust of Canada ("CATC") (together, "Computershare Canada") are Canadian federally incorporated trust companies licensed under the Trust and Loan Companies Act. CATC is a subsidiary of CTCC. Their ultimate parent company, Computershare Limited ("CPU") is an Australian financial services company with worldwide business operations and considerable experience in the financial services industry.

Policies, Frameworks and Guidelines for Operational Risk Management

Computershare Canada manages operational risk through an enterprise-wide Operational Risk Framework that forms part of the broader Computershare Limited Enterprise Risk Management (ERM) Framework. The framework is designed to provide a structured, consistent, and forward-looking approach to identifying, assessing, managing, monitoring, and reporting operational risks across all Canadian business units and legal entities.

The framework is aligned with the principles of the Committee of Sponsoring Organizations of the Treadway Commission (COSO) and considers ISO 31000:2018 Risk Management Guidelines, with adaptations to reflect Canadian regulatory expectations applicable to federally regulated financial institutions. Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people, systems, or external events.

Operational risk management is embedded into strategic planning, capital planning, business operations, and change initiatives, and is supported by a comprehensive risk library covering financial and non-financial risks. The framework integrates governance, risk, control, compliance, and resilience activities to support the achievement of business objectives while protecting reputation, customers, and stakeholders.

Key supporting components include:

- A comprehensive operational risk taxonomy embedded in the enterprise risk library;
- Formal risk identification, assessment, and treatment standards;
- Defined risk appetite statements, thresholds, and metrics;
- Standards governing operational risk event management, change risk and third-party risk;
- Regular stress testing and scenario analysis, which assists in the evaluation of downside risks during strategic, capital and business planning;

- Assessment of Pillar 1 and Pillar 2 risks on a quarterly basis (or more frequently as required), and an Internal Capital Adequacy Assessment Process (ICAAP) on at least an annual basis;
- Linkages to business continuity, disaster recovery, and resilience capabilities, supporting operational resilience outcomes aligned with OSFI expectations.

Structure and Organization of Operational Risk Management

Computershare Canada applies a Three Lines of Defence model that clearly defines roles, responsibilities, and accountabilities for operational risk management.

- **First Line of Defense – Risk Ownership**

  Business units and functional teams are accountable for identifying, assessing, managing, and reporting operational risks inherent in their activities. Risk owners are assigned for each material risk and are responsible for the design, implementation, and operation of controls, as well as remediation of control weaknesses and escalating risks that exceed appetite or tolerance.

- **Second Line of Defense – Independent Risk Oversight**

  The independent Risk function, led by the Chief Risk Officer (Canada), establishes operational risk management standards, provides oversight and challenge of first line activities, reviews risk assessments and metrics, monitors adherence to risk appetite, and escalates material issues to senior management and the Board Risk and Audit Committee.

- **Third Line of Defense**

  Internal Audit provides independent assurance over the effectiveness of the operational risk framework, governance, and control environment, reporting directly to the Board Risk and Audit Committee.

Operational Risk Identification, Assessment, and Measurement

Operational risk measurement at Computershare Canada combines qualitative and quantitative techniques supported by formal systems, data, and governance processes.

Operational risks are identified and assessed through structured processes including Risk and Control Self Assessments (RCSAs), process mapping, analysis of audit findings, review of operational risk events and near misses, and consideration of emerging risks. Risks are assessed using standardized likelihood and consequence criteria, covering financial, regulatory, reputational, customer, and people impacts.

Inherent risk, residual risk, and calculated risk ratings are determined using defined risk matrices. The effectiveness of controls is considered through assessments of design adequacy and operating effectiveness. Operational risk events and loss events, including actual losses, potential losses, and near misses, are captured, analyzed, and trended to support risk measurement, root cause analysis, and continuous improvement. Operational risk exposure is monitored through Key Risk Indicators (KRIs) linked to risk appetite.

CTCC and CATC are categorized as Category III SMSBs, and as such the simplified risk-based capital ratio (SRBCR) methodology is used to determine capital requirements. The Simplified Risk-Based Approach is used to calculate Adjusted Total Assets and Operational Risk Weighted Assets for Pillar 1 Capital. Pillar 2 Capital is based on management's assessment of risks and internal assessment of stress testing. The ICAAP is prepared in accordance with OSFI's CAR Guideline.

Reporting and Escalation Framework

Operational risk reporting is embedded within Computershare Canada's risk governance and oversight structure and supports effective decision making at all levels of the organization.

Regular reporting includes business unit risk status updates to the Chief Risk Officer, consolidated reporting to the Canada Risk Forum, and escalation of material operational risks to the Senior Management Committee and the Board Risk and Audit Committee. High and extreme residual risks, risks outside of appetite, significant operational incidents, and emerging risk themes are subject to enhanced governance and oversight.

Out-of-cycle escalation and reporting are undertaken when significant operational risk matters arise to ensure timely management attention and Board awareness.

Risk Mitigation and Risk Transfer

Computershare Canada manages operational risk through a structured risk treatment framework. Risk treatment options include risk mitigation through preventive and detective controls, risk acceptance within defined authority and appetite, avoidance of activities with unacceptable risk exposure, transfer or sharing of risk with third parties (including through insurance coverage where appropriate), and contingency planning for critical operations.

Controls are documented in accordance with established standards and are assessed for both design adequacy and operating effectiveness. Control weaknesses and operational risk findings are tracked through formal findings management and remediation processes. Where appropriate, residual operational risk exposure may be mitigated through insurance or other risk transfer mechanisms.

The operational risk framework also underpins Computershare Canada's operational resilience capabilities, supporting continuity of critical operations through disruption and alignment with supervisory expectations for operational resilience.