Briefing
Compliance News Affecting Pension Plans
February 2026

Risk-Management Guideline for Plan Administrators

The Canadian Association of Pension Supervisory Authorities (CAPSA) released its Risk-Management Guideline, which replaces and consolidates previous guidance on specific types of risks pension plan administrators face, including:

- Third-party advisors or service providers
- Cybersecurity
- Investment governance
- Environmental, social and governance (ESG) factors
- Use of leverage in plan investments

The guideline defines the key elements of a risk-management framework and sets out the principles to identify, evaluate, manage and monitor material risks. Proper implementation of a risk-management framework will ensure plan administrators and trustees fulfill their fiduciary obligations and standard of care.

Four-step process for risk management

Step one: Identify risks

Plan administrators should identify and document the risks to which the plan may be exposed. These risks may include but are not limited to:

- Asset/liability mismatch
- Intergenerational equity
- Longevity
- Litigation
- Information technology and cybersecurity

Segal

The plan's documentation should also include the controls that are in place or could be put in place to reduce the severity and/or likelihood of the identified risks materializing.

Step two: Evaluate risks

Once risks have been identified, plan administrators are expected to develop a process for evaluating and prioritizing the risks according to the overall threat they pose to the plan. Material risks to the pension plan should be quantified.

Risk-assessment tools available to plan administrators include, but are not limited to, heat maps, sensitivity analysis, stress testing and stochastic modeling.

Properly evaluating risks should help ensure that sufficient resources are directed to priority areas of material risks.

Step three: Manage risks

Once risks have been identified and evaluated, plans can begin implementing controls to prevent, detect and mitigate risk.

These controls include:

- Disaster-recovery plans
- Contingency plans
- Financial policies
- Insurance
- Training and education
- Member communications
- External audits

The controls implemented should be suitable for the nature of the risk and proportionate to its likelihood and severity.

Once controls are in place, the plan administrator should also determine any residual risks and whether to avoid these risks, implement additional measures to mitigate these risks or transfer to a third party.

Step four: Monitor risks

Plan administrators should continuously monitor risks as well as review the controls implemented in step three. To properly evaluate the effectiveness of the controls in place, plan administrators should consider information drawn from audit reports, valuation reports, administrative and investment reports.

Risk management is a continuous process. Steps one through three should be repeated at regular intervals to ensure the risk-management framework continues to be effective.

Considerations for specific risks

Third-party risk

To perform specific tasks, plan administrators often retain the services of third-person service providers, such as lawyers, accountants, actuaries, third-party administrators and investment advisors. However, even if a third-party service provider is engaged, plan administrators retain their fiduciary duty and are responsible for the oversight and management of the plan.

Examples of third-party risk scenarios include:

- Insolvency of the third party
- Loss of data by the third party
- Operational disruption at the third party

Plan administrators should incorporate the management and monitoring of third-party risk into their risk-management framework. The responsibilities of all third-party providers should be documented and controls put in place to monitor their compliance with the administrator's overall governance framework.

Some key considerations when establishing an approach to third-party risk include:

- Does the third-party appointment process include performance indicators?
- Does the plan administrator ask third-party advisors informed questions to verify the reasonableness of their advice?
- Is due diligence taken prior to contracting with third-party service providers?

Cybersecurity

As a fiduciary, plan administrators must ensure that proper controls are in place to protect plan beneficiaries and plan assets against the risk of cyberattacks. They should have a plan in place to respond to, recover and report cyber incidents.

Examples of cyber risk include:

- Malware
- Phishing emails
- Inadvertent information disclosure

Some key considerations when integrating cyber risk into the plan's risk-management framework include:

- Does the plan administrator have sufficient training, skills and expertise to adequately understand and manage cyber risk?
- Have all critical technology assets been identified?
- Does the plan administrator have adequate cyber insurance?
- Are controls in place to minimize the risk of a cyber incident as well as its potential impact?
- Has the plan administrator reviewed cyber-risk management of its third-party service providers?

Plan administrators should work with all relevant parties to determine:

- How cyber incidents will be detected
- How the plan will recover from an incident and restore normal operations
- What disclosures should be made with respect to an incident

Additionally, plan administrators should be familiar with any reporting requirements of their pension regulator.

Investment-risk governance

Plan administrators are expected to invest the assets of a pension fund with the degree of care that a person of ordinary prudence would exercise in dealing with the property of another person.

Plan administrators act as stewards and should use their position as owner to influence the activity or behaviour of investee companies, investment managers, information officers or other market participants in ways that reflect the plan administrator's views about managing risks.

There are a wide range of investment risk-management practices available to plan administrators, including:

- **Portfolio limits.** Plan administrators may include a maximum exposure to each asset class in the plan's statement of investment policy and procedures (SIP&P).
- **Risk-based sensitivity limits.** These limits link investment portfolio sensitivities to changes in key risk factors, such as market risk.
- **Value-at-risk (VaR).** VaR quantifies the impact of a range of expected market shocks. The range of outcomes should be consistent with the plan's risk appetite.
- **Stress testing and asset-liability modelling.** Stress testing includes sensitivity testing, scenario testing and reverse stress testing. It is intended to simulate the impact of possible shocks on the plan's investments.
- **Practices for alternative assets held by the pension fund.** Plan administrators should consider the risks that arise when investing in alternative investments, such as private equity, private debt and derivatives. These investments are susceptible to misvaluation risk given the limited data available. Plan administrators should perform due diligence with respect to any valuations of alternatives from third-party investment managers before making an investment.

ESG issues

ESG information can be material in assessing a plan's risk-return profile. Plan administrators should consider ESG risks when developing plan governance, risk management and investment decision-making practices.

Governance processes should ensure the plan administrator:

- Assigns responsibility for considering the materiality of ESG risks for inclusion in the plan's risk-management framework
- Keeps pace with developments in the market regarding ESG practices, as well as industry standards, legislation and regulatory policy
- Assesses its own ESG knowledge and experience and obtains third-party expertise as needed to meet their standard of care

The severity and timing of ESG risks can be difficult to predict, making risk models based only on historical information limited. Plans should consider scenario analysis to assess any vulnerabilities of the pension fund.

Disclosure of ESG considerations is a regulatory requirement in most jurisdictions:

- Minimum standards pension legislation in all Canadian jurisdictions requires the SIP&P to include a description of factors relevant to investment policies and procedures, including, in some cases, ESG considerations.
- When ESG information is considered, best practice suggests that the plan administrator disclose this information to plan stakeholders.

Use of leverage

Leverage occurs when a strategy that increases a plan's economic exposure to investment assets beyond what it could achieve beyond normal investment of its capital in securities.

Commonly used method of leverage used by pension plans include:

- Financial leverage involves plan's accessing additional funds to invest. The funds may appear as liabilities on the plan's balance sheet.
- Synthetic leverage occurs when a pension plan enters into derivatives contracts.
- Embedded leverage involves exposure acquired indirectly through a plan's holdings of third-party managed investments.

Plan administrators must be aware of the risks associated with leverage. These include:

- **Market risk.** Leverage can increase market risk by amplifying losses.
- **Liquidity risk.** This occurs primarily through the inability to convert assets to cash without losses.
- **Counterparty risk**. Plans that invest in derivatives or repurchase agreements enter into contractual relationships with other parties. The risk of loss due to the counterparty's unwillingness or inability to meet its contractual obligations is counterparty risk.

Pension plans that use leverage must implement processes and procedures to manage these risks including:

- Setting appropriate risk tolerances for the plan
- Adopting investment objectives and approaches that are consistent with those risk tolerances
- Establishing oversight procedures that effectively identify, evaluate, manage and monitor exposures and risks
- Reporting of the above to those responsible for plan governance

Pension plans that use leverage should document their policies and procedures regarding leverage in their SIP&P. Specifically, plans should document:

- The objectives of using leverage, with respect to risk and expected return
- How leverage is to be used to achieve the plan's objectives
- The types of leverage the plan will or may use and the plan's guidelines that apply to its use
- How leverage affects and fits into the plan's broader investment approach; its strategic asset allocation
- How the plan administrator will oversee the use of leverage

Plan administrators should have systems in place to monitor and manage how leverage affects the risks facing the plan as well as how the risks due to the use of leverage are to be measured and monitored.

Next steps

Plans should operate in accordance with CAPSA guidelines, which outline industry best practices. However, plans should also consider whether their pension regulator may specify its own expectations.

Segal can be retained to work with plan sponsors and their legal counsel on determining the implications. For assistance or if you have questions about the regulations and the law, contact your Segal consultant or get in touch via our website.

To receive future issues of Segal's *Briefing* and other publications, join our email list.

Follow us:

Segal