Guideline No. 10

Guideline for Risk Management for Plan Administrators

September 9, 2024

Table of Contents

SECTION 1: INTRODUCTION AND CONTEXT

The Canadian Association of Pension Supervisory Authorities (CAPSA) is publishing this Guideline to support pension ***plan administrators*** in fulfilling their fiduciary duties and in considering their legislated standard of care.

The primary purpose of a pension plan is to provide lifetime retirement income to the ***plan beneficiaries***. When administering the plan and investing pension plan ***assets***, plan administrators must act in accordance with their fiduciary duty in fulfilling this purpose. Good risk management is a key characteristic of a well-run pension plan and an important part of the plan administrator's role in protecting ***plan members'*** benefits. An effective framework for managing risk will assist plan administrators in keeping plan assets safe, protecting the plan from adverse risks, and supporting the plan in meeting its objectives.

As such, CAPSA determined it appropriate to define the key elements of a risk management framework and, in consultation with the industry, set out principles to: identify, evaluate, manage, and monitor ***material risks***. This Guideline outlines overarching principles of risk management and risk considerations for specific topics, including *Third-Party Risk; Cyber Security Risk; Investment Risk Governance; Environmental, Social, Governance Risk;* and *Use of Leverage* (see Section 7).

This Guideline is intended to complement CAPSA Guideline No. 4: Pension Plan Governance, as well as other CAPSA Guidelines that refer to risk management (for example, Guideline No. 7: Pension Plan Funding Policy).

Key Takeaways from this Guideline
• The plan administrator should create a risk management framework to identify, evaluate, manage, and monitor material risks. • The plan administrator should review the risk management framework regularly. • The design of each pension plan's risk management structures and practices will vary based on the plan's characteristics and circumstances and the risks being assumed.

Please note that defined terms are *italicized* and **bolded** when first used. Definitions are in the Glossary of Terms, contained at the end of the Guideline.

SECTION 2: SCOPE

This Guideline is intended for all pension plan administrators of ***defined benefit***, ***defined contribution***, ***pooled registered***, ***target benefit,*** or ***hybrid plans***.

Once a pension plan is established, the plan must be administered, and its assets invested, by the administrator as a fiduciary, with the skill, care, and diligence required by the standard of care set by the governing pension legislation. The establishment and implementation of a risk management framework to identify, evaluate, manage, and monitor risks facing the plan can be an important element in fulfilling the required standard of care. Pension regulators may periodically review the risk management framework prepared by the plan administrator to assess whether the plan administrator is fulfilling its fiduciary duty and meeting the standard of care.

2.1 Proportionality and Complexity Considerations

A priority for CAPSA is to ensure that this Guideline is relevant and helpful for all pension plans, regardless of factors like the plan type, the complexity of its ***administration*** and investment strategies, and the size of the plan membership and plan assets. It is acknowledged that the method of implementing some of the concepts in this Guideline may differ from one pension plan to another. Plan administrators are encouraged to adapt their risk management practices to reflect the plan's investment beliefs, specific circumstances, and risks.

When designing a risk management framework, plan administrators should consider the circumstances of their pension plan, including the operational risks and complexity of the plan's strategies. For example, plans with significant in-house or directly-managed investment activities should consider separating duties between those responsible for operational activities (e.g., investment and administration) and those responsible for oversight activities (e.g., development of risk management policies and procedures and assessing whether the plan's ***risk tolerances***, ***risk limits***, ***controls***, and timeliness of reporting and escalation are adhered to). This separation of duties creates an independent risk oversight, which mitigates the potential for conflicts that could arise if both functions were carried out by the same individual or group.

SECTION 3: WHAT IS RISK MANAGEMENT?

Plan administrators face an ever-changing and increasingly complex risk landscape. A systematic approach can help plans to effectively identify and manage their risk exposure.

Risk management involves:

- establishing sound governance and oversight commensurate with the pension plan's complexity and size;
- establishing processes and methodologies for identifying, evaluating, managing, and monitoring risks that may adversely impact a pension plan's ability to operate as intended and deliver benefits to plan beneficiaries; and
- establishing effective controls (in the form of systems, procedures, or arrangements) to understand, manage, and mitigate those risks.

Principle 7 of CAPSA Guideline No. 4: Pension Plan Governance states: "*The plan administrator should establish and document a framework and ongoing processes, appropriate to the pension plan, to identify and manage the plan's risks*." In the context of a pension plan, a risk management framework and process should help identify risks, including in the following areas:

- the way the plan is governed, managed, and administered (including the use of third-parties);
- the way the plan assets are invested;
- the way the plan's liability, funding, and benefit adequacy are managed; and
- the way the plan communicates with members.

To be effective, risk management should consider the long-term nature of pension obligations, but also consider the short-term risks. While risk management is an important consideration for plan administrators in fulfilling their fiduciary duty and standard of care, it is also an important consideration for ***plan sponsors.***

Both the plan administrator and plan sponsor may benefit from better understanding the risks impacting each other. For example, where the plan sponsor is responsible for any funding deficiency in the plan, it should consider, based on the current funding and investment strategy, the potential range of future plan funding contributions and its ability to withstand a potential significant increase in funding requirements.

These considerations may inform the plan sponsor's own risk assessment in terms of its tolerance for managing fluctuations in its contribution requirements and ability to continue to fund the plan and discharge its corporate fiduciary duty.

Considerations regarding the Plan Sponsor
• Plan sponsors may have different stakeholders than the plan administrators (e.g., shareholders). • Plan administrators and plan sponsors need to work together to identify and manage risks to achieve the shared goal of offering a pension plan. • At times, the plan administrator and plan sponsor may be the same entity. Where this is the case, the plan administrator should consider the potentially conflicting responsibilities and how it will resolve any conflicts that arise by virtue of its dual role.

SECTION 4: DEFINING OVERALL RISK

In order to implement a process to identify, evaluate, manage, and monitor a plan's risks, the plan administrator should first establish, in the form of a written statement, an overall ***risk appetite, risk tolerance,*** and ***risk limits***, and incorporate these into the governance and risk management frameworks for the plan.

Risk appetite is the amount and type of risk that the plan administrator is able and willing to accept while meeting their fiduciary duty.

Risk tolerance is the variation in outcomes that the plan administrator can accept for a given risk. Risk tolerance may differ for different risks, based on operating environment, stakeholders, etc., but must be clearly understood by the individuals making risk-related decisions on a given issue.

Risk limits represent thresholds that should not be exceeded based on the plan's ***risk appetite statement***. Risk limits help to ensure that risks are effectively managed and that they align with the plan's risk appetite and risk tolerance.

Considering how to incorporate risk appetite, risk tolerance, and risk limits into the governance and risk management frameworks is both integral and a prerequisite step to constructing those frameworks.

SECTION 5: RISK MANAGEMENT FOUR-STEP PROCESS

A plan sponsor's decision to offer a pension plan to their employees is a voluntary one. In establishing and designing the plan, the sponsor should identify the objectives (i.e., desired outcomes) of the plan and communicate them to the plan administrator. The plan administrator should also identify its specific objectives for the plan in relation to fulfilling its fiduciary duty to the plan's beneficiaries.

For example, what are the objectives for members' benefit security (e.g., a higher benefit that is less secure vs. a lower benefit that is more secure), predictability (e.g., replacement income target), and affordability (e.g., level and variability of contribution rates)? With defined and documented objectives, the plan administrator can then implement risk management practices to increase the likelihood that the objectives are met.

5.1. Step One: Identify Risks

The identification of risks provides an opportunity for plan administrators to consider and record all risks to which the plan may be exposed. There are a wide range of risks that may be relevant to pension plans. In identifying risks, plan administrators may want to consider information drawn from several sources, including but not limited to:

- audit reports;
- actuarial reports;
- service provider contracts;
- complaints;
- relevant court cases and decisions;
- administration and investment reports; and
- publications about external emerging factors that are likely to impact the plan investments and administration.

Some risks may have immediate impacts, such as those arising from inaccurate member information or a cyber or data security incident. Others may be realized over a longer period, such as the impact of climate change on plan investments. It is important to understand that risks, both immediate and prolonged, may be interrelated, correlated, or cumulative. Risk identification should therefore also examine the interaction between different risks and consider their interconnectedness. See Appendix A: Risk Table for a sample of possible risks facing a plan.

Plan administrators should document the risks identified and, for each risk, the stakeholders that are impacted. Many pension plans record all risks identified in a risk register and review it regularly (i.e., at least annually). A risk register provides a template to record risks, as well as opportunities facing the plan, and may also include an assessment of the implications of the risks identified. A risk register should also document the controls that are or could be put in place, to reduce the severity and/or likelihood of risks materialising and to record factors that could indicate a change in the level of risk identified.

Recording risks helps to formalize risk management procedures and provides plan administrators with a central reference point for ease of reporting. Here is an Example Risk Register from the downloadable trustee toolkit published by the Pensions Regulator, the regulator of workplace pensions in the United Kingdom.

Many larger plans in Canada have a risk committee with a dedicated focus on the governance of risk identification, assessment, and prioritization.

5.2. Step Two: Evaluate Risks

Having identified risks, plan administrators should develop a process, based on the nature, size, and complexity of the plan, for evaluating and prioritizing the risks according to the overall threat that they pose to the plan's viability and their potential impact on the plan's stakeholders. Risks should be considered separately and in combination.

One common way of evaluating and prioritizing risks is to evaluate the potential severity of the risk against its probability of occurring by using a heat map approach. See Appendix B: Sample Heat Map.

A variety of other risk assessment tools exist, which can be helpful in developing a sound approach to risk management and evaluating risks. If a more sophisticated approach is needed, using a more advanced risk assessment tool, or several tools in combination, can also be helpful. Plan administrators should consider the tools appropriate to their plans. Common financial risk assessment tools can be found in Appendix C: Risk Assessment Tools.

The prioritization of risks based on likelihood and potential severity will dictate the extent to which mitigating action should be taken. This will be dependent upon a number of factors, including plan administrator judgement and the risk appetite statement. A risk categorized as having high likelihood and high severity requires more immediate and focused attention as it represents a significant threat to the plan.

Risks that are material to the pension plan should be quantified. Monitoring material risks, as determined by their potential severity and likelihood, together with appropriate contingency planning, will allow plan administrators to respond quickly and effectively should the risks materialize.

Whichever method of evaluation the plan administrator chooses, it should help ensure that resources are directed to priority areas of material risks.

5.3. Step Three: Manage Risks

Simply recording and evaluating risks does not necessarily result in risks being managed. As part of the risk management process, plan administrators should implement suitably designed controls to manage risks.

Controls are an essential component of plan governance and help protect members' benefits. The purpose of controls is to prevent, detect, and mitigate errors, irregularities, and fraud and to mitigate other types of risk. Controls may take many forms, including but not limited to:

- financial policies (e.g., investment policy, funding policy);
- reviews or performance evaluations;
- disaster recovery plans;
- contingency plans;
- training and education;
- policies on priority issues (e.g., conflicts of interest or climate change);
- insurance;
- external audit by properly qualified professionals; and
- communications to members.

Plan administrators should establish controls to mitigate and manage plan risk as part of their fiduciary obligations and standard of care. The controls that the plan administrator puts in place should be suitable for the nature of the risk and proportionate to its likelihood and potential impact. Plan administrators should measure the effectiveness of their controls. Failure to implement effective controls with respect to a known material risk could constitute a breach of the plan administrator's standard of care.

Once controls are in place for a risk, the plan administrator should determine the remaining (residual) risk, if any, based on their risk limits and decide whether to: accept the residual risk; avoid the risk; respond to the risk by implementing further mitigation measures; or transfer some or all of the risk to a third-party.

A sound approach to risk management involves considering what could be done should risks materialize, with a particular emphasis on contingency planning. This can also help to identify opportunities to reduce plan risk.

No two risks are the same and plan administrators should exercise judgement when seeking to mitigate risks. For example, it can be the case that the costs of implementing a control exceed the possible costs to address the risk should it materialize. Of course, cost may not be the only consideration when deciding on controls.

A risk management framework should give the plan administrator reasonable assurance that plan operations are performed properly, and controls are in place to detect (and correct) errors when they occur, including in areas with respect to any delegated authority and areas where the plan may be vulnerable to risks. It is important to note that, although plan administrators may delegate certain tasks to third-parties (such as investment consulting), the plan administrator retains fiduciary responsibility.

A risk management framework that clearly articulates the accountability for the management of a pension plan's operations and the related risks helps plan administrators meet their fiduciary and other responsibilities, including the requirement that pension assets are invested prudently.

Plan administrators should consider some form of independent review of the adequacy of the risk management framework put in place.

5.4 Step Four: Monitor Risks

The ongoing monitoring and review of risks and the risk management framework and controls is a key component of managing risk.

In performing ongoing monitoring of risks and controls, plan administrators should consider information drawn from various available sources, such as audit reports, member surveys, valuation reports, and administration and investment reports.

Risk management is an iterative rather than a one-off exercise. The plan administrator should repeat the risk identification and evaluation steps at intervals (proportionate to circumstances of the plan) to identify ***emerging risks*** or opportunities.
The risk management framework and controls should be evaluated regularly to ensure they continue to be appropriate and effective.

SECTION 6: SUMMARY

A robust risk management framework supports plan administrators in fulfilling their fiduciary obligations including appropriate consideration of their applicable standard of care.

As outlined in this Guideline, all pension plans, regardless of plan type, size, or assets, should follow good risk management practices. Doing so assists plan administrators in:

- better understanding the risks facing the plan, and how those risks could prevent the plan from meeting its objectives;
- understanding how risks are interconnected and how risks could simultaneously impact the plan's outcomes; and
- mitigating risks through appropriate tools and controls.

Pension regulators may periodically review the risk management framework prepared by the plan administrator to assess whether the plan administrator is fulfilling its fiduciary obligations and standard of care. This may include reviewing:

- the risk management framework generally; and
- high priority risks and how they are being managed and monitored by plan administrators.

Consistent with the principle of proportionality, plan administrators are encouraged to adapt their risk management practices to reflect the plan's specific circumstances and the risks they face.

SECTION 7: RISK CONSIDERATION FOR SPECIFIC TOPICS

As highlighted in Section 2.1 of this Guideline, a priority for CAPSA is to ensure the information is relevant and helpful for all pension plans, regardless of factors like the plan type, the complexity of its administration and investment strategies, and the size of the plan membership and plan assets. CAPSA acknowledges that some of the concepts in this section may not be applicable or feasible for all pension plans or that application may differ from one pension plan to another.

Plan administrators are encouraged to adapt their risk management practices to reflect the plan's investment beliefs, specific circumstances, and risks.

7.1 Third-Party Risk

7.1.1 Background

Plan administrators often rely upon the services of external parties, or third-party service providers, to carry out numerous activities for the plan (e.g., administration, investment, actuarial valuations, and audits), including to perform specific tasks or to supplement the skills and knowledge of the plan administrator.[1] In the context of a pension plan, typical third-party service providers include, among others, independent professionals (e.g., lawyers, accountants, third-party administrators, ***actuaries***, and investment consultants).

It is important that plan administrators understand that, while services and responsibilities may be delegated to third-party service providers, the plan administrator retains their fiduciary duties and remains responsible for the oversight, management, and administration of the plan. This section builds upon CAPSA's foundational guidance on plan governance, CAPSA Guideline No. 4: Pension Plan Governance, by focusing on the specifics of third-party risk as a key consideration in pension plan management.

Plan administrators can refer to Section 7.2.4 for managing third-party ***cyber risks***.

7.1.2 What is Third-Party Risk?

Third-party risk is the risk to the plan's operational and financial resilience or reputation due to a third-party failing to provide goods and services, protect data or systems, or otherwise carry out activities in accordance with the arrangement.

[1] As established in *CAPSA Guideline No. 4: Pension Plan Governance*, a third-party service provider is defined as: the entity (or entities) or individual(s) that is/are retained by the plan administrator to perform some or all of the delegated duties associated with the pension plan and the pension fund that the plan administrator is required to perform.

Examples of third-party risk scenarios include:

- a plan administrator over-relying on advice received from third-party advisors (e.g., failing to verify the reasonableness of such advice or not prudently monitoring and managing third-party relationships);
- insolvency of the third-party or a material subcontractor;
- operational disruption at the third-party due to human error, inadequate or failed processes and systems, or from external events (e.g., cyber incidents); and
- loss of data by the third-party.

7.1.3 Integrating Third-Party Risk in Governance and Risk Management

Plan administrators should incorporate the management and monitoring of third-party risk into the same governance and risk management frameworks used to assess and respond to other material risks to the plan.

Due diligence is essential to monitor third-party service providers' compliance with the plan administrator's overall governance framework and all regulatory requirements. Steps should be taken by plan administrators to clearly define and document third-party responsibilities, and to implement effective oversight.

Third-party risk is a risk for all plan administrators engaged in third-party delegation. The plan administrator's approach to monitoring and managing third-party risk should be regularly reviewed (e.g., on an annual basis) and modified, as required, so that appropriate controls are always in place to allow the plan administrator to manage the risk.

As with other risks, appropriate controls vary depending on the nature, potential impact, and likelihood of the risk at issue.

Key Considerations for Third-Party Risk
Plan administrators should consider the following types of questions, as they establish and evaluate their approach to third-party risk. This list is not exhaustive, and a plan's specific situation should be considered. • does the plan administrator understand that it retains its fiduciary duties and remains responsible for the oversight, management, and administration of the plan, regardless of any delegation to third-parties that may occur? • does the third-party appointment process include performance indicators for third-parties and a system to manage third-parties? • does the plan administrator ask third-party advisors (e.g., lawyers, actuaries, or investment consultants) informed questions, to verify the reasonableness of the advice being received? • is due diligence undertaken prior to entering contracts (including service level agreements) with a third-party proportionate to the level of risk and criticality of the arrangement?

- is due diligence undertaken in the process of appointing third-parties, so that appointments are free of actual or perceived conflicts of interest?
- is due diligence undertaken as part of the contract renewal process and on an ongoing basis, whenever there are material changes to the third-party arrangement?
- are third-party arrangements supported by a written contract or other agreement that sets out the rights and responsibilities of each party?
- does the plan administrator have visibility into the use of subcontractors, and are subcontractor services taken into consideration in the management of third-party risk?
- does the plan administrator scrutinize the reasonableness of fees associated with third-party services and whether these fees are reflective of the market?

7.2 Cyber Security

7.2.1 Background

As plan administration and asset management increasingly rely on technology, there is a growing need for plan administrators to address cyber risk to keep plan assets safe and protect the rights and interests of plan beneficiaries.

Plan administrators and their third-party service providers control substantial amounts of financial assets as well as personal and confidential data, which can make them an attractive target for criminals, cyber-attacks, and fraud. Cyber breaches may have far-reaching consequences for plan beneficiaries and their families, as well as causing reputational damage to the parties involved.

A pension plan must be administered, and its assets invested by the plan administrator as a fiduciary, in accordance with the legislated standard of care. Steps therefore should be taken to protect plan beneficiaries and plan assets against the risk of cyber-attacks. This is a key risk that all plan administrators and their agents should be aware of and actively monitor and manage. A plan administrator should implement the expectations outlined in this Guideline relative to the size of the plan; the nature, scope, and complexity of its operations; and its risk profile.

7.2.2 What is Cyber Risk?

Cyber risk is the risk of financial loss, operational disruption, or reputational damage from the unauthorized access, malicious and non-malicious use, failure, disclosure, disruption, modification, or destruction of information technology systems and/or the data contained therein. In the context of a pension plan, cyber risk includes both internal risks (e.g., disgruntled employees or a lack of controls on access) and external risks (e.g., hacktivists, state-sponsored threat activists, or cybercriminals).

Examples of cyber risk include:

- malicious software (also known as malware);
- phishing emails (i.e., acquiring sensitive data through a fraudulent solicitation, in which the perpetrator masquerades as a legitimate business or reputable person);
- hacking (i.e., obtaining unauthorized access to networks, computer systems, and digital devices); and
- inadvertent information disclosure (e.g., the accidental leaking of private member information).

7.2.3 Integrating Cyber Risk Management

To effectively integrate cyber risk management, plan administrators should consider some of the characteristics that make managing cyber risk challenging. These include the evolving nature of technology, cyber practices, and data standards; the need for specialized technological expertise and training; and the sensitive nature of information retained by plans

that may have long-term implications in the event of disclosure (e.g., identity theft) and which can lead to loss of trust and reputational risk.

Plan administrators should recognize cyber risks and be aware of their fiduciary duty to manage these risks. Appropriate controls vary depending on the nature, potential impact, and likelihood of the risk at issue.

Key Considerations for Integrating Cyber Risk

In integrating cyber risk into a plan's governance and risk management frameworks, the plan administrator should consider the following questions:

- are the roles and responsibilities in respect of the plan administrator's approach to cyber risk clearly defined and documented?
- does the plan administrator have in place sufficient training, skills, and expertise to adequately understand and manage cyber risk?
- has the plan administrator identified its critical technology assets (e.g., software or hardware) and access management (i.e., the framework of policies and technologies used to authenticate user access) and data protection frameworks?
- is there a sufficient understanding of the potential impact of a cyber incident as well as the likelihood of different types of breaches occurring?
- is there an understanding of the extent of the plan's cyber exposure, including that arising from the actions or inactions of third-parties?
- is there a discussion of third-party cyber risk management with third-party service providers (at both the onboarding phase and regular intervals)?
- are cyber risks appropriately identified, and are they reviewed regularly, including when there are significant changes to the plan's operations? Does the review include metrics that track the efficacy of the responses to cyber incidents?
- are existing controls sufficient and proportionate to minimize the risk of a cyber incident as well as its potential impact?
- does the plan administrator have in place an appropriate cyber insurance policy and, if so, what is covered by the insurance (e.g., incident response)?
- does the plan administrator have another governance approach or policy in place that may overlap with cyber security?

7.2.4 Managing Third-Party Cyber Risks

Cyber risk should be an active consideration in the selection of a third-party service provider and suitable provisions should be included in contracts.

The plan administrator should satisfy itself that all third-party service providers have implemented sufficient controls to protect plan beneficiary data and plan assets.

7.2.5 Planning for the Incident and Response

Cyber risks generally involve an “incident” and a “response”. Plan administrators must build their cyber resilience – meaning, the ability to assess and minimize the risk of a cyber incident occurring, and also the ability to recover when an incident takes place. To ensure effective management of an incident, plan administrators should work with all relevant parties (including those performing in-house functions, third-party service providers, and employers) to determine:

- how cyber incidents will be detected;
- how the plan will recover from an incident and restore normal operations (see Section 7.2.6); and
- what disclosures should be made, and to whom, with respect to an incident (see Section 7.2.7).

7.2.6 Resiliency Plans

Management of cyber risks may include establishing resilient contingency plans to deal with incidents and to resume operations swiftly and safely. The core elements of a resiliency plan would typically address business continuity, disaster recovery, and incident response. A resiliency plan should cover a range of scenarios and the likelihood of different types of incidents. Key considerations include:

- the roles and responsibilities of the incident response team, including third-party responsibilities and their incident response processes;
- the resources required to investigate the cyber incident and maintain critical functions (e.g., payments of benefits) and processes;
- in-crisis communications, including how and when reporting will be made to board members or trustees (as applicable); and
- the process, thresholds, and time limits for notifying other parties including the supervisory authorities, law enforcement (in cases of fraud), third-parties, and where necessary, plan beneficiaries.

Plan administrators may also benefit from creating a cyber breach playbook covering various potential scenarios and conducting regular simulation exercises with all relevant parties, employees, third-party vendors and service providers, outsourcing companies, etc., to practice and improve cyber incident management capabilities. Plan administrators should implement the expectations regarding resiliency plans relative to their plan’s size; the nature, scope, and complexity of its operations; and its risk profile.

7.2.7 Incident Reporting

Regarding incident reporting, plan administrators should:

- be familiar with the privacy/data security legislation that applies in the plan's jurisdiction;
- be clear on how and when cyber incidents should be reported to the plan administrator, to plan beneficiaries, and to other appropriate parties;
- determine whether notification of a cyber incident to other parties is required, either voluntarily or as prescribed by any legislation, and comply with reporting requirements including materiality within prescribed timelines;
- inform plan beneficiaries about any cyber incident that has an impact on their benefits, or financial or personal interests; and
- communicate to affected plan beneficiaries the measures being taken to mitigate the impact of these incidents and, if appropriate, steps plan beneficiaries should take to monitor for any irregularities resulting from the breach.

7.2.8 Evolving Nature of Cyber Risks

Cyber risks are complex, rapidly evolving and require a dynamic response, therefore:

- controls, processes, and response plans should be regularly tested and reviewed;
- plan administrators should stay up to date on cyber risks; and
- plan administrators and other relevant parties should seek appropriate information and guidance on cyber security threats to enhance their ability to respond to, and recover from, cyber incidents.

Key Considerations for Cyber Security:
• Cyber risk is a key risk for all plans, regardless of plan size or characteristics. It should be regularly reviewed and assessed, and appropriate controls should be in place to allow the plan to manage the risk. Cyber risks are complex and evolving and require a dynamic response. • in fulfilling their fiduciary responsibilities, plan administrators should have access to the required skills, expertise and/or training to understand and manage cyber risk. • roles and responsibilities relating to cyber risk should be clearly defined, assigned, and understood, including with respect to any activities delegated to third-party service providers (and all applicable subcontractors). • plan administrators should have a strategy in place for responding to and reporting cyber incidents.

7.3 Investment Risk Governance

7.3.1 Background

Pension standards legislation in Canada requires that the administrator of a pension plan invest the assets of the pension fund with the degree of care that a person of ordinary prudence would exercise in dealing with the property of another person. In addition, the plan administrator is required to employ the knowledge or skill that they possess or ought to possess by reason of their profession or business.

Key Considerations for Investment Risk Governance
As highlighted in Section 4 of this Guideline, defining the plan administrator's risk appetite establishes the guiding principles from which the plan's administrative policies and processes are subsequently developed. Identifying the categories and level of investment risk that the plan administrator is willing or expected to take in order to meet the pension promise ensures that the plan's ***statement of investment policies and procedures (SIP&P)*** and investment strategies are consistent with the plan's objectives and overall risk appetite, mitigating the impact of unexpected market shocks that could place members' benefits at risk.

Stewardship
Plan administrators undertake stewardship, as appropriate to their plan size, design, and investment beliefs, as a part of prudent investment decision-making. Stewardship activities involve a plan administrator seeking to use their position as owner or creditor to influence the activity or behaviour of investee companies, asset owners, investment managers, information officers, or other market participants in ways that reflect the plan administrator's views about risks and opportunities and how to manage them.

Plan administrators' stewardship expectations are often reflected in a set of voting principles/policies. By documenting their approach to voting (e.g., in developing their own proxy voting principles and/or adopting the proxy voting guidelines of their investment managers), plan administrators facilitate discipline in their voting activities and provide transparency to plan stakeholders.

For plans relying on third-party investment managers to integrate stewardship considerations into the plan's investment activities (including member-directed investments), principles for prudent delegation apply, including to articulate and document the plan's stewardship expectations in the service-provider agreement.

7.3.2 Considerations for Plan Administrators with Less Complex Investment Strategies

Plan administrators should assess the circumstances of their pension plan including the operational risks and complexity of their investment strategies.
For plans with less complex investment strategies (such as some that rely on third-party investment managers, or those that invest exclusively in pooled funds), the following may constitute an appropriately robust risk management governance structure:

- implementing more frequent governance self-assessments;[2]
- separating the duties of the operational and risk management functions where it is impractical to separate oversight to different members of a pension committee or governing body (documented in the governance framework); and
- commissioning periodic third-party reviews of the plan administrator's operational and risk management practices.

As Section 7.1 of this Guideline explains, accountability for any risk management functions delegated to third-party service providers rests with the plan administrator – the plan administrator is not discharged of its fiduciary duties and oversight responsibilities when relying on third-party service providers. The plan administrator must take steps to mitigate and manage these risks including due diligence performed during the hiring process, ongoing monitoring, and periodic performance assessments.

7.3.3 Investment Risk Management Practices

There are a wide range of investment risk management practices available to plan administrators. Their utility will depend on the complexity of the plan administrator's investment strategy and risk appetite. Several of the more widely used practices include portfolio limits, risk-based sensitivity limits, stress testing, and asset liability modelling. In addition, special considerations may apply in respect of plans that hold alternative investments.

Portfolio Limits
Many plan administrators augment the asset mix policy set out in the plan's SIP&P with portfolio limits. Limits are typically defined as maximum and minimum exposures to each asset class or sub-class, whether as a percentage of the portfolio's holdings or based on a debt issuer's credit quality.

Since the asset mix policy effectively functions as a target, portfolio limits serve an important risk management function such that breaches trigger timely review of the investment strategy to mitigate the risk that the plan inadvertently exceeds its risk appetite. To function as an effective control mechanism, portfolio limits should be set to identify and review all material deviations from the plan's investment policy. A limit breach does not necessarily require that action be taken to rebalance the portfolio, however repeated breaches may cause the plan

[2] CAPSA recommends that plan administrators complete the *Pension Plan Administrator Governance Self-Assessment Questionnaire* at least annually.

administrator to determine whether changes to the risk appetite statement and SIP&P are required.

Risk-Based Sensitivity Limits

While portfolio limits can be a simple and effective risk management tool, they do not directly measure the impact of key risk factors. Risk-based ***sensitivity limits*** are types of risk limits that link investment portfolio sensitivities to changes in key risk factors (e.g., market risk, interest rate risk, etc.). However, portfolio limits may be sufficient for plans with less complex investment strategies.

Defining risk-based sensitivity limits serves an important risk management control function by helping plan administrators:

- understand the plan's sensitivity to shocks to material market risk exposures; and
- ensure that the potential impact of these risk exposures does not exceed the plan's overall risk appetite.

Plan administrators should establish appropriate limits based on historical sensitivities to material risk factors consistent with the plan's overall risk appetite. A plan administrator monitors the plan against these limits to ensure that the risks to which the plan is exposed pursuing its investment strategy continue to fall within the plan's overall risk appetite.

The use of sensitivity limits will not influence the probability that an unexpected market shock that exceeds the plan's risk appetite will occur. Rather, the value of sensitivity limits lies in informing plan administrators regarding the risks inherent to their chosen investment strategies, to identify market shocks whose impact exceeded the expected range and by initiating discussions regarding risk and reward including adjustments to risk appetite, investment policy, or investment strategy as appropriate following outsized shocks.

Value-at-risk (VaR) is a metric that quantifies the impact of a range of *expected* market shocks, typically over a period of one year. Value-at-risk can be measured as an asset-only volatility, or it can be adapted to measure the volatility of the funded position of the plan (sometimes referred to as "Surplus-at-Risk"). The range of potential outcomes should be consistent with the plan's risk appetite. Plan administrators frequently manage their plans with the objective of maintaining a fully funded status (i.e., benefit security) or to mitigate funding volatility (i.e., management of employer's contributions). In such cases, the risk appetite or the sensitivity limit may be based on the maximum decrease (volatility) of the plan's going-concern or solvency position that the plan administrator is willing to accept.

Sensitivity limits should be reviewed periodically to ensure that the thresholds remain appropriate and provide for diversification and correlation among related risk factors. Sensitivity limits should be consistent and applicable at different levels of authority under the plan's governance framework. The limits should be linked to the plan's risk appetite and address all material risk exposures.

A breach of a sensitivity limit should be subject to immediate review by the plan's risk and operational management functions and escalated by the independent risk management function when appropriate (e.g., when breaches are significant or repeated). If the breach is determined to be transitory in nature or the plan remains within its overall portfolio risk appetite, no change to the plan's risk appetite or investment strategies may be warranted and the risk management function may approve a temporary bulge limit increase. Any approval limit increases must be in line with the delegation of authority for the breached limit as set out in the governance framework. The plan administrator should also review the plan's risk appetite to ensure that it remains appropriate in light of current market conditions.

Stress Testing and Asset Liability Modelling

Stress testing and asset liability modelling (ALM) are tools used to identify and manage investment risks, develop the SIP&P, and formulate long-term investment strategies. They facilitate the identification of key risk factors and quantify the impact on the plan's objectives (e.g., going-concern or solvency position, contribution levels and volatility) of a change in one or more risk factors. Stress testing, which may include ***sensitivity testing, scenario testing*** and ***reverse stress testing***, simulates the impact of a range of plausible shocks and scenarios on the plan's investment and funding policies. Stress testing results thus serve as a useful tool to inform the process of selecting and calibrating sensitivity limits linked to the plan's key risk exposures. ALM assists the plan administrator in managing asset-liability mismatch risk and aligning investment strategies with the plan's risk appetite by modelling the impact of changes to key risk factors.

Plan administrators are expected to use stress testing and ALM as appropriate for the circumstances and key risk factors relevant to each plan. When used to assess investment strategies against the plan's risk appetite and limit risk exposures, stress testing and ALM assist the plan administrator in discharging its fiduciary duties and fulfilling its obligation to invest pension assets prudently.

Practices for Alternative Assets Held Directly by the Pension Fund

In contrast to liquid securities traded on a public exchange, alternative investments, including private market equity and debt securities, derivatives and real assets transacted over-the-counter, are particularly vulnerable to misvaluation risk. This risk is particularly sensitive during periods of increased market volatility. Unlike public securities whose valuations are easily marked to market, valuations of alternative investments are frustrated by limited availability of market data. Valuations of real estate, frequently subject to highly localized market conditions, often require specialized market expertise. Plan administrators should therefore consider the risks that arise when investing in alternative assets, for instance, the increased risk during periods of market volatility due to misvaluation risk and liquidity risk.
Plan administrators should incorporate into the governance framework their processes and controls that provide for appropriate and independent valuation of alternative assets to ensure these are fairly valued.

Plan administrators often rely on valuations carried out by third-parties to assess the value of pension fund assets. Prior to investing in assets that require valuations, plan administrators should perform sufficient due diligence with respect to the valuation methodology, including the

frequency of valuation, to ensure that it is consistent with the plan's objectives, risk appetite and investment philosophy.

Independent interim valuations may be appropriate during periods of market volatility to ensure that the plan's financial statements reflect the fair market value of the plan's assets. However, it is often impractical for a plan administrator to obtain an independent interim valuation. As a result, plan administrators should account for some degree of asset value uncertainty that may arise during periods of market volatility.

Plan administrators should develop, document, and approve valuation methodologies that clearly define the processes to ensure that pension fund assets are fairly valued. Due diligence should be performed with respect to any valuations sourced from third parties, including a review of the investment policies and methodologies used by third-party investment managers both before making an investment and periodically thereafter. Plan administrators should ensure that disclosures relating to third-party valuations are sufficient to enable them to fully understand and address any shortcomings.

7.4 Environmental, Social, Governance (ESG) Issues

7.4.1 Background

Environmental, Social and Governance (ESG) information can be relevant to performing an assessment of a pension fund's risk-return profile by enabling an expanded view of factors that might affect the value of pension plan assets and liabilities.

7.4.2 Fiduciary Duty in the Context of ESG

When administering the pension plan and investing pension plan assets, plan administrators must act in accordance with their fiduciary duty in fulfilling the primary purpose of the plan - providing retirement income.[3]

Using ESG information to provide financial insight is consistent with an administrator's fiduciary duty. Conversely, ignoring or failing to consider ESG information that might materially affect the fund's financial risk-return profile could be a breach of fiduciary duty. How plan administrators assess and respond to ESG information will vary depending on plan circumstances, including plan design, size, extent of reliance on external asset managers, and investment beliefs and strategies. Plan administrators will also have to consider cost-efficiency, as risk-adjusted returns are prudently assessed on a net-of-fees basis.[4]

[3] In Canada, Income Tax Regulations, subsection 8502(a) states that "the primary purpose of the plan is to provide periodic payments to individuals after retirement and until death in respect of their service as employees." For more information on fiduciary duty, see CAPSA Guideline No. 4 – *Pension Plan Governance Guideline*.
[4] For example, in the context of passive investments, plan administrators may decide these strategies offer competitive investment management costs and align with their investment beliefs about the efficiency of public markets to account for material information, including ESG information.

Principle 1
Pension plan administrators (either directly or through their delegates) should consider whether and how ESG information may be material to assessing the financial risk-return profile of their fund and take appropriate action.

7.4.3 Implementing ESG Information

As ESG issues and techniques for assessing and responding to ESG issues are expected to continue to evolve, prudent governance, risk management and investment practices will need to be adaptive and regularly reviewed to assess emerging gaps, risks and opportunities.

Principle 2
Plan administrators, as part of their standard of care, should design their plan governance, risk management and investment decision-making practices to identify and respond to material ESG risks and opportunities in a manner appropriate for their plan's circumstances and investment beliefs. A review should be conducted regularly and whenever there is a material change in the risks facing the plan or governance processes.

7.4.4 Governance

CAPSA sets out general expectations with respect to plan governance in Guideline No. 4: Pension Plan Governance. Concerning ESG risks, 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; and
- assesses their own ESG knowledge and experience and obtains third-party expertise as needed to meet their standard of care.

Third-party expertise can include:

- actuaries and investment and risk management professionals, who can assist with understanding ESG risks and opportunities, reviewing existing practices and identifying appropriate responses; and
- legal advisors, who can assist with understanding fiduciary duty, the appropriate use of ESG information, and providing disclosure to plan stakeholders.

As part of its governance activities, plan administrators may find it beneficial to develop, and record in written policies, a set of investment beliefs about ESG information and its application to the plan's financial risk-return profile. The beliefs can be included in the statement of investment policies and procedures (SIP&P), other relevant policies (e.g., external manager

selection and due diligence frameworks, and policies regarding stewardship) or as a stand-alone document.

7.4.5 Risk Identification and Evaluation

Risks identified by ESG information should be considered together with other types of risks incorporated into the plan's risk profile or when evaluating and making plan investment decisions. Some characteristics complicate the identification, evaluation, management and monitoring of ESG risks. These include:

- longer time horizons for those risks to fully emerge;
- interrelatedness/correlation with other risks;
- limited or incomplete information, difficulties with quantification;
- variation in the availability of ESG information by asset class;
- modelling complexities; and
- evolving reporting and management standards and practices.

These challenges underline the importance of having governance processes to keep current with developments in the market. Third-party resources, such as ESG rating agencies and standard-setting entities, can be an aid to understanding and verifying ESG risks within portfolios.

ESG risks have been described as "transverse" in that they can manifest through other risks, such as market, credit, insurance, operational, reputational, and legal risks.
Certain ESG risks, for example biodiversity loss, human environmental damage, social inequality, loss of social cohesion, and in particular climate change, have been described as systemic.

Among ESG issues, climate change is considered to pose urgent and material systemic risks to the financial system[5]. The physical and transition[6] risks associated with climate change are expected to increase over time. These risks can potentially affect short-term and long-term investment returns, but also create opportunities for investment (e.g., in new technology or in companies that better mitigate their existing exposures to physical and transitions risks). These risks might also affect plan liabilities to the extent that discount rates are affected or if, for example, extreme weather events (floods, wildfires, heat etc.) affect present or future mortality and morbidity rates overall or in specific localities.

While the types of climate risk are foreseeable, the magnitude, timing, and specific pathways of these risks can be difficult to predict. Risk models based only on historical information are therefore limited. Where appropriate to plan circumstances, scenario analysis can be a useful

[5] Systemic risks cannot be avoided through diversification.
[6] Physical risks include rising sea levels, increased flooding, extreme heat events and wildfires. Transition risks are those risks associated with transitioning to a low carbon economy and include increasing disclosure requirements, shifting asset values, changes in consumer preferences and changes in regulations, technology, and business practices.

exercise for plan administrators (and/or investment managers) to assess the vulnerabilities of the pension fund or an investment strategy under different plausible forward-looking risk scenarios, including over different time horizons. Scenario analysis can also be used to incorporate and assess potential effects of changes in plan liabilities.

Understanding the range of analytical outcomes can lead to a better understanding of a plan's funding risks, informing the plan's investment, assumption-setting, and funding decisions.

7.4.6 Investment Decision-Making

Investment Strategy
Establishing investment limits or targets may be helpful to understand and manage ESG risk exposures and operationalize ESG investment beliefs.
Periodic evaluation can help determine whether such limits or targets are delivering on their intended outcomes and keeping pace with developments in understanding ESG risks and mitigation practices.

Prudent Delegation and ESG Integration
To the extent that a plan administrator delegates investment management to a third-party asset manager or provider of OCIO (outsourced chief investment officer) services, prudent delegation will require the plan administrator to understand whether and how ESG information is integrated into the governance, risk management and investment decision-making processes of the asset manager or provider and whether these processes are consistent with the plan administrator's investment beliefs and risk profile.

Member Choice Plans
For defined contribution plans that provide members with choice in selecting investments, plan administrators may determine it is consistent with their fiduciary duty to include in the plan's investment line-up both traditional funds which integrate ESG information as well as "ESG-related funds". Plan administrators should monitor and determine whether the inclusion of such funds remains consistent with their fiduciary duty.[7]

If a decision is made to include an ESG-related fund, the plan administrator can demonstrate prudence by describing the rationale for the selection of the ESG-related fund(s) to help plan members understand the investment objective, the risk-return characteristics of the fund, and how the fund can be incorporated into an investment portfolio from among the investment options in the plan line-up.

[7] An "ESG-related fund" is a fund whose investment objectives reference ESG information or a fund that uses ESG strategies (see CSA Staff Notice 81-334 – ESG-Related Investment Fund Disclosure). Legal and investment advice can assist plan administrators in understanding any potential risks associated with including such a fund or funds in the investment line-up. Risks could include the effect of (a) the fund's mandate on investment performance relative to alternative investment options, and (b) providing too much investment choice to plan members (i.e., complicating decision making for plan members and increasing their information needs for investing in such a fund).

Stewardship
Stewardship, as described in Section 7.3.1 of this Guideline, by plan administrators directly or through their investment managers or industry associations can be a prudent way to exercise influence to minimize ESG risks.

7.4.7 Disclosure

Stakeholders have an interest in knowing that plan administrators are appropriately identifying and responding to relevant risks and opportunities, including whether and how ESG information is considered. Pension standards legislation in all jurisdictions require the plan's investment policy (e.g., SIP&P) to include a description of factors relevant to investment policies and procedures. Disclosure of ESG considerations may be a regulatory requirement in some jurisdictions.

When ESG information is considered for governance, risk management and investment purposes, best practice suggests that the plan administrator disclose this as part of information regularly shared with plan stakeholders.

Where the plan administrator relies on a third-party investment manager to take ESG information into account in managing plan assets, the plan administrator can reference its adoption of the manager's ESG policy or describe the plan administrator's considerations with respect to ESG information in its selection, ongoing supervision and review of the manager.

Where the plan administrator takes a more direct and active approach with respect to ESG information, the plan administrator is encouraged to keep pace, as appropriate for its circumstances, with industry best practices regarding disclosure, including descriptions of:

- the roles and responsibilities of the administrator or its agents in identifying and managing ESG risks;
- the materiality and relevance of specific ESG risks to the plan; and
- any stewardship activities undertaken.

The disclosure standards of the Canadian & International Sustainability Standards Boards (CSSB & ISSB) may be helpful resources in this regard.

Principle 3
As a best practice, plan administrators should describe, in a level of detail proportionate to its circumstances, whether and how material ESG information is considered and refer to that information in its investment policy or in other sources of plan information, such as websites, fund facts or statements.

7.5 Use of Leverage

7.5.1 Background

Leverage can amplify the potential gains and losses on investments and increase exposures to other investment-related risks. Using leverage therefore increases the importance of managing risk.

For the purposes of this section, leverage exists when any technique or strategy is used to increase a pension plan's economic exposure to investment assets beyond what it could achieve by simply investing its capital (or net assets) in securities or other financial assets. In other words, leverage is a means of achieving economic exposure greater than the capital invested.[8]

Some common purposes for which pension plans are known to use leverage include:

- **implementing Liability Driven Investment (LDI) strategies**. To increase a pension plan's exposure to assets that behave like the plan's liabilities.
- **increasing exposure to return-seeking assets**. For example, this may be achieved using balance sheet leverage or "synthetic" leverage using derivatives contracts.
- **seeking investment efficiencies and opportunities available through leverage**. For example, increased diversification and the ability to take larger positions in low-volatility asset classes.

7.5.2 Types of Leverage

Common types of leverage for pension plans include:

- **financial leverage**, which involves a plan accessing additional funds to invest. The funds may appear as liabilities on the plan's balance sheet or be associated with specific investments, such as mortgages on real estate.
- **synthetic leverage,** which occurs when a pension plan enters into derivatives contracts that, for example, may allow the plan to increase exposure to fixed income or return-seeking assets.
- **embedded leverage,** which includes any form of leveraged investment exposure acquired indirectly through a plan's holdings of third-party managed investments (i.e., leverage not directly created at the pension fund or pension plan level). Embedded leverage is the most common type of leverage for most plans.[9]

[8] While leverage is commonly used to increase economic exposure, synthetic leverage in derivative contracts can also be used to decrease or hedge economic exposure and mitigate certain risks. Such use is also subject to the risks described in Section 7.5.3.

[9] This is because most pension plans invest predominantly in pooled funds rather than directly, and do not employ financial leverage or engage heavily in derivatives transactions at the plan level to increase economic exposure.

Various types of leverage differ with respect to their terms and conditions. One important distinction is whether the leverage is "recourse" or "non-recourse":

- **non-recourse** generally limits the plan's exposure to the amount invested.
- **recourse** refers to the possibility that a counterparty may demand that the plan pay additional amounts from the fund to cover losses that exceed the amount invested.

This distinction has important implications for the level of risk linked to the leverage and how these risks are managed by the plan.

7.5.3 Risk Associated with Leverage

This section describes key risks that need to be considered in the context of a plan's use of leverage. A list of common risks and their definitions can also be found in Appendix A: Risk Table**.** Plan administrators need to be aware of how these risks may interact with each other.

Market Risk
Leverage can increase market risk by amplifying losses. Leveraged investment strategies can also change how market risk impacts other risks to which the plan may be exposed. For example, in certain leveraged strategies, short-term changes in the value of assets may increase liquidity risk.[10]

In general, the potential impact of leverage on market risk needs to be considered from the perspective of both the plan's assets as well as the plan's liabilities.

Liquidity Risk
Liquidity risk is the risk that the pension plan may not be able to meet short-term financial obligations or may not be able to meet those obligations without incurring undue losses. These obligations include those arising from the use of leverage. This risk usually occurs due to the inability to convert assets to cash without losses.

Plan administrators that employ leverage need to understand how it impacts liquidity requirements and risk. This will depend on the types of leverage involved and the purposes for which it is used. For example, liquidity management is critical to certain LDI strategies that employ leverage using derivatives.[11] Since margin agreements associated with leverage strategies often require the maintenance of a certain level of liquid assets, an increase in market volatility or credit deterioration may cause liquidity pressures on plans employing leverage.

[10] For example, when a pension plan uses repurchase agreements to obtain additional funds to invest, changes in the quality of the pledged securities can make it more difficult to roll over the agreements and impact the plan's liquidity needs.
[11] As these strategies require a sufficient supply of eligible and unencumbered collateral instruments to allow the plan to meet calls for additional collateral as required.

Counterparty Risk
Leverage achieved using certain instruments, such as derivatives or repurchase agreements, involves contractual relationships with other parties (i.e., counterparties). Counterparty risk is the risk of loss due to a counterparty's unwillingness or inability to meet its contractual obligations when they come due.

Mechanisms exist to mitigate the risk of loss in such circumstances. These include "global netting agreements" with parent companies that allow the set-off of obligations across a parent and its subsidiaries[12]. Employing these types of mechanisms is part of the prudent management of counterparty risk.

Other Risks
Other risks that may apply to pension plans using leverage are operational risk, refinancing risk, model risk and performance measurement risk.

7.5.4 Leverage Risk Management Practices for Plan Administrators

If a pension plan uses leverage, the plan administrator's standard of care requires a sound understanding of how leverage affects investment risks and prudent use of leverage.
The processes and procedures that a plan administrator puts in place for managing these risks must reflect the types of leverage involved and whether leverage is at the pension plan or fund level or embedded in pooled funds or other investments.

Leverage is at the pension plan or fund level: The pension plan's risk management framework must include the operational controls necessary to manage the plan's use of leverage.

Leverage is embedded in pooled funds or other investments: The plan administrator is expected to have sufficient information and understanding of the leverage used by the funds in which the pension plan invests. The information should be sufficient to assess the impact on the plan's risks and manage them effectively.

[12] For example, pension plans should strive to have global agreements with each parent counterparty that allow for netting with all its subsidiaries, rather than bilateral agreements with each subsidiary individually. In the absence of global agreements, the plan may have difficulty settling offsetting amounts in a market or credit event.

Key Considerations for Leverage Risk Management Practices
• 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; • assessing capacity and competency to oversee its use of and exposures to leverage; and • reporting of the above to those responsible for governance (e.g., senior management and the board of directors/trustees)

7.5.5 Prudent Use and Oversight of Leverage

A high degree of complexity is involved in implementing leveraged strategies. Plan administrators that do not have the required expertise may seek advice from external experts when assessing, implementing, and managing leveraged strategies. A plan administrator that relies on external experts is not discharged of its fiduciary duties and oversight responsibilities and it must assess its capacity and competency to oversee its use of and exposures to leverage. Plan administrators should consider CAPSA Guideline No. 6: Prudent Investment Practices with respect to prudent investment practices, including delegation.

Decisions about use and type of leverage must be consistent with the plan administrator's investment objectives, risk appetite, and risk tolerance. The plan administrator should also ensure the use of leverage is consistent with the plan's SIP&P and other relevant policies. The rationale behind leverage-related decisions should be thorough and well-documented and should address:

- decisions about whether to use leverage;
- setting appropriate guidelines and controls;
- the type(s) of leverage used; and
- the purposes for which it is used.

Metrics that specifically measure the amount of leverage and/or its effects can provide plan administrators with additional insights for the prudent use and oversight of leverage. CAPSA recognizes that no single metric provides a comprehensive measure of all dimensions of leverage risk, that the measurement of leverage is complex and that approaches to understanding and measuring leverage continue to evolve.

For plans that adopt leverage measurement metrics, the plan administrator should ensure that:

- the plan's investment managers that use leverage are familiar with leverage measurement issues and techniques, including the illustrative metrics;
- the plan actuary or risk management team can quantify the plan's risk exposures, including leverage; and
- those responsible for governance have or obtain appropriate expertise to understand and oversee leverage use and risk.

7.5.6 Documentation

When a plan uses leverage, it should document its policies and procedures regarding leverage in the plan's SIP&P. The SIP&P disclosure should include at minimum a broad description of the plan's objectives in using leverage, in relation to:

- the plan's overall investment strategy;
- the asset/liability interactions and funding objectives; and
- specific investment strategies and activities.

The SIP&P or other policies of the plan[13] should establish appropriate guidelines and controls related to the use of leverage. These should be aligned with the plan's overall risk appetite, risk tolerance, and risk management framework. As appropriate for the kinds of leverage used by the plan, the guidelines should describe the process for identifying, monitoring, and reporting the risks associated with leverage. Controls should include strategies for managing or mitigating identified risks.

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, and other aspects of the investment portfolio; and
- how the plan administrator will oversee the use of leverage. This includes monitoring and controlling various risks that may arise or be impacted by its use.

7.5.7 Integrating Risk Management

Plan administrators should put in place appropriate systems to monitor and manage the use of leverage;

- how leverage affects the risks facing the plan; and
- how risks arising from leverage are to be measured and monitored.

Expectations for risk management may be different for administrators of plans that use leverage directly compared to indirectly.

In the case where a plan invests in a pooled fund that employs leverage, the plan administrator should understand how leverage is being employed. A good practice for plan administrators is to identify, in the plan's processes for monitoring the use of leverage, material instances of embedded leverage and its effects on associated risks. At a minimum, the pension plan's

[13] Depending on the size and complexity of investments and the extent of direct management by the plan relative to externally managed funds, plans may find it appropriate to establish more detailed risk guidelines and controls for leverage in other policy documents.

investment risk metrics should reflect any risks to the pension plan implied by the pooled fund's leverage.[14]

Performance and risk benchmarks should incorporate and reflect the use of leverage to promote a more informed and consistent measurement of these parameters.

7.5.8 Identifying and Managing Risk

Stress testing and ***scenario analysis*** provide mechanisms for understanding and managing the implications of leverage for the plan's broader investment approach and the funding of its liabilities.

Stress testing and scenario analysis can help pension plans establish appropriate parameters and limits on general investment risk. They can also help establish parameters and risk limits on specific investment activities and strategies, including those using leverage.

Plan administrators should conduct stress testing of their portfolios, including leveraged strategies, under various market conditions and scenarios. The full impact of the use of leverage, including resulting investment risks, should be incorporated into the plan's stress testing.

Plan administrators that use leverage should also consider enhancing their stress testing to incorporate a reverse stress test.

Plan administrators should consider appropriate measures to mitigate risks associated with investment strategies that involve the use of leverage. Robust netting agreements, the use of central counterparties, and the posting of collateral are examples of mitigation of counterparty and market risks.

[14] Under extreme market stresses, leveraged positions could significantly affect the value of the pooled fund. Plans should understand the vulnerabilities of the pooled fund to extreme market stresses in assessing the riskiness of the pooled fund investment and the effect of such a change in value on the plan's overall investment and funding. Diligence into the manager's stress testing activities and contingency plans can inform the plan about risks in the ability of the pooled fund to absorb changes in value to leveraged positions under extreme market stresses.

APPENDIX A: RISK TABLE

The following list outlines common risks faced by a plan administrator in the operation of a pension plan. The list should not be seen as comprehensive.

Risk	Description
Funding Risks	
Funding	The risk that a pension fund does not have sufficient assets to meet its liabilities on either a going-concern or solvency basis. For an ongoing plan, this could result in additional special payments to amortize any deficiencies, or benefit reductions, including reductions to accrued benefits, if applicable. For a plan termination, depending on the plan type and reason for termination, members' benefits will be at risk of not being fully funded.
Asset/Liability Mismatch	The risk arising from movements in interest rates, bond prices, stock and commodity prices, exchange rates, etc., having a differential effect on plan assets and liabilities. For example, a drop in interest rates that increases the value of liabilities by more than the increase in the value of assets.
Model	The risk associated with a model not accurately capturing and quantifying the liabilities and assets (and their associated volatilities), resulting in inappropriate strategic decisions, such as selecting an inappropriate asset mix.
Intergenerational Equity	The risk that different generations of plan members experience different outcomes (pension benefits or contribution costs) that are perceived as unfair, because of poor plan design, funding, or decision-making. For example, in a target benefit plan, increases to the provision for adverse deviation (PfAD) owing to a conservative funding policy could result in active members experiencing diminished benefit accruals, whereas retired members enjoy enhanced benefit security and stability.
Liability / Pension / Actuarial Risks	
Actuarial Methods and Assumptions	The risk of inappropriate actuarial valuation methods (e.g., smoothing methods) and assumptions (e.g., expected return on assets, mortality assumptions) resulting in overestimating or underestimating liabilities or asset values.
Annuity Timing	The risk of higher annuity prices due to interest rates at the time annuities are purchased.

	For a defined benefit or target benefit plan that is de-risking or winding up, this could result in annuities costing more than the fund assets can cover. For a defined contribution plan, this could result in less purchasing power for members who annuitize during a time with especially low interest rates compared to others who annuitize at a more favourable time, with higher interest rates resulting in lower pricing.
Longevity	The risk that members live longer than expected based on the actuarial assumptions. For a defined benefit plan, this could result in experience losses and increased funding requirements. For a target benefit plan, this could lead to benefit reductions and potential intergenerational inequity. For a defined contribution plan, the risk is that members might outlive their retirement savings (where an annuity is not chosen at retirement).
Investment Risks	
Investment Strategy	For defined benefit or target benefit plans, the risk that the investment strategy of the plan is not properly aligned with its fiduciary responsibility, risk appetite and tolerance, or long-term investment or target income replacement goals, and therefore, negatively affects the achievement of the plan's long-term objectives. For defined contribution plans, the risk that the types of investment options made available to members (where there is investment choice) are not sufficient or appropriate to satisfy the members' individual investment risk appetite and long-term investment or target income replacement goals.
Liquidity	The risk that a pension plan will be unable to obtain the necessary funds (i.e., have sufficient cash) to meet payment obligations as they fall due or will be unable to meet payment obligations without incurring excessive costs or unacceptable losses. Liquidity risk is most present in mature plans (where pension payouts are more likely to exceed contributions) and in plans using significant hedging and/or leverage strategies.
Credit/Counterparty	The risk that an issuing entity in which a plan invests, or a counterparty with which it interacts, will be unable to fulfill its obligations, adversely affecting the plan's investments or member confidence in the pension plan.

Concentration	The risk that a pension fund's portfolio is not adequately diversified and too exposed to one asset class, geography, or issuer.
Foreign Currency Exchange	The risk that investments made in a foreign currency will be subject to volatility in the foreign currency exchange rate (and hence the carrying value in local currency), in addition to other asset-related investment risks.
Market	The risk of unexpected adverse market investment performance of the pension fund. Poor market investment performance may lead to lower defined contribution account balances than expected or underfunding of defined benefit plans due to a shortfall of plan assets relative to plan liabilities. This may increase the contributions required to meet benefit obligations or require retirement benefits to be adjusted accordingly. Market risk is broad and can be affected either directly or indirectly by movements in the equities market, bond market, interest rates, foreign currency, inflation, etc. A plan's asset allocation will be one of the primary factors affecting its exposure to market investment risk (e.g., if an investment portfolio is not sufficiently diversified and is too concentrated on one asset class). Market risk can also be systemic in nature when all pension plans are affected by financial downturns or other economic events.
Refinancing	The risk that a plan will incur a financial loss because it is unable to replace an existing debt obligation required to maintain its leveraged investment positions, without undue cost. A pension plan can experience refinancing risk from internal factors (e.g., the deterioration of its credit rating) or external factors (e.g., adverse interest rate movements or tightening credit market).
Environmental, Social, and Governance	The risk that action or inaction related to environmental, social, or governance factors may negatively impact the value of an investment asset in the future.
Performance Measurement	The risk that the increased volatility of returns and resulting tracking errors caused by leverage may not be appropriately captured by a plan's performance and risk benchmarks.
Valuation	When investing in private market assets, valuation risk is the risk of mispricing an asset's value given that these assets are not traded in a liquid, public market exchange and require reliance on professional judgement and limited data. In particular, valuation risks are heightened during periods of market volatility.
Governance Risks	

Governance	Risks related to gaps in the oversight of the plan's operation and management, leading to a breach of fiduciary duty. Gaps can exist due to plan administrators not receiving adequate training, having insufficient knowledge or skills to fulfill their duties, being provided with insufficient or inadequate information and materials from service providers, having conflicts of interest in decision-making, etc.
External and Strategic	The inherent risks regarding the sensitivity of the fund to external factors. These risks arise from adverse strategic decisions, improper implementation of decisions, or lack of responsiveness to changes in the surrounding environment. These include risks related to demographics, competition, technology, conjuncture, interested parties, infectious disease, and political stability. Strategic risks include the continued viability of a plan when there is a change in the operating environment, including an internally driven change such as a merger or the coverage of a new group of participants in the pension plan with potentially significantly distinctive characteristics and challenges.
Operational Risks	
Information Technology (IT) and Cyber Security	The risk arising from inadequate information technology and processing in terms of manageability, exclusivity, integrity, infrastructure, controllability, and continuity. IT risk also arises from poor IT strategy and policy and from inadequate use of information technology. Cyber security risks arise from insufficient, failed, or vulnerable IT infrastructure or software, inadequate policies or policy compliance gaps, and user errors, resulting in the exposure of personally or organizationally sensitive data, or losses due to disruptions in operations.
Litigation	The risk to the plan administrator of members suing them because of real or perceived negligence, errors, or broken promises, arising from member communications, administration, or investment management. This can lead to financial costs to the administrator or loss of member confidence in the pension plan.
Operational	The risk of losses resulting from inadequate internal processes, people, and systems – whether these are performed in-house by the plan administrator or delegated to a third-party service provider. Operational risk includes administration risk, which includes the following: • failure to enroll eligible employees;

	• errors in calculations of contributions and benefits; • inaccurate member data (service, salary, hours worked, beneficiary records); • failure or delays in paying members' benefits. These risks often arise due to inadequate controls or processes in place for effective administration. Operational risk also includes the risk of loss due to external events, such as fire, natural disasters, burglary, or theft.
Fees/Expenses	The risk of unfavourable variability in fees or expenses charged by service providers (e.g., custodians, investment managers, consultants, third-party administrators) and paid from plan assets (or, in the case of defined contribution plans, from the members' accounts).
Legislation	The risk that public policy or political decisions that directly affect the pension plan are not anticipated or negatively impact the plan's ability to meet its original objectives.
Disinformation/ Misinformation	The risk of relying on false information that is shared, either intentionally (disinformation) or unintentionally (misinformation), exacerbated by the widespread use of generative artificial intelligence and large language models as search tools to produce content.
Communication	The risk arising from a failure to provide members with education and adequate, understandable communication about their benefit entitlements. For example, the risk of not disclosing investment options for a defined contribution plan can result in compliance issues, financial losses, legal liabilities, and or loss of member confidence in the plan. For target benefit plans, the risk of plan members not understanding the variable nature of their benefit can result in legal action against the plan administrator or loss of member confidence in the plan.
Regulatory/ Compliance	The risk of adverse consequences arising from the misinterpretation of or failure to comply with all relevant laws and regulations.
Plan Sponsor Risks	
Plan Sponsor	The risk that a plan sponsor is not able to meet its contribution obligations to the plan, or to continue to sponsor the plan over the long-term, leading to a plan wind-up. This can result, for example, in benefit reductions if a defined benefit plan is not fully funded on a solvency basis, or for a defined contribution plan, exposing members to annuity timing risk. Other risks related to the plan sponsor can arise, for example:

	• a business decision to amend, close or wind-up the plan; • a significant change in the workforce (downsizing, slowing growth), compared to the current or past demographic composition of the plan; • for target benefit (TB) plans, levels of employment or member work hours may materially decrease, exposing members to contribution risk, given the fixed nature of contributions.
Participating Employer	For a multi-employer plan, the risk arising from the concentration of a significant portion of the plan's membership in a single employer. The withdrawal of such an employer from the plan could have a significant impact on the plan, for example, an increase in contributions or a benefit reduction (in a target benefit plan) for the remaining participating employers and members. There is the risk of employer delinquency where participating employers do not remit contributions in accordance with the terms of the plan and/or collective agreement.
Emerging Risks	
Emerging	A risk which may develop, or which may already exist, that is difficult to quantify or may have a high loss potential. Emerging risks typically have very long-time horizons and may develop slowly but mitigating actions may also take a long-time to implement and become effective.

APPENDIX B: SAMPLE HEAT MAP

After identifying the risks that may impact the plan, the plan administrator could use a heat map such as the one below to determine which risks are most important to prioritize. Each risk is rated on a scale of 1 to 4 for its likelihood of occurrence and for its severity, in the context of the plan and based on qualitative and quantitative scoring criteria. These two ratings are then multiplied together to determine where the risk is on the heat map (and the level of overall concern). A risk with a likelihood of occurring of 1 and a severity of 1 has a risk rating of green, that is, low. On the other hand, a risk with a severity of 4 and a likelihood of 4 has a risk rating of red, indicating that the risk should be prioritized.

A risk categorized as having high likelihood and high severity will require focused attention as it represents a significant threat to the plan. Further monitoring and controls for such a risk should be considered.

Example Heat Map

Severity					
	4	4	8	12	16
	3	3	6	9	12
	2	2	4	6	8
	1	1	2	3	4
		1	2	3	4
		Likelihood			

Example – Cyber security: While the plan already has robust cyber security protections and training in place, it is recognized that cyber security incidents are increasingly common and difficult to prevent. Considering the existing controls, the plan administrator rates the likelihood of a cyber security incident as moderate to high (i.e., 3). In addition, because the plan retains sensitive data for the purpose of benefit payments (e.g., Social Insurance Numbers), it rates the potential severity of a cyber security incident as high (i.e., 4). The combined rating is therefore 12, corresponding to a risk rating of red. The risk should be prioritized.

APPENDIX C: RISK ASSESSMENT TOOLS

Risk assessment tools can be helpful in developing a sound approach to risk management. When deciding on risk assessment tools to use, plan administrators should bear in mind the principles of proportionality, as sophisticated risk assessment tools may be time-consuming and costly, and not necessary if the risks facing the plan are simple and straightforward. Following is a list of common financial risk assessment tools. Other risk assessment tools exist.

Sensitivity analysis: Sensitivity analysis involves identifying variables that affect the finances of the plan (e.g., interest rates, inflation, equity returns), changing the values for those variables in isolation, and seeing what effect this has on the plan objectives. This helps identify which variables are most important.

Scenario testing: Scenario testing involves changing the values of several variables simultaneously at a single point in time, in a way that is internally consistent and reflects a chosen economic scenario.

Scenario projections: While sensitivity analysis and scenario testing consider the effect of an immediate change in conditions, scenario projections help understand how the plan's finances may evolve in future years. Projection models vary in points of detail, and some can be quite complex.

Stress testing: Stress testing involves performing a projection under a scenario of significantly adverse conditions for the plan, which may be the result of several risk factors materializing, or a severe occurrence of just one risk factor, over a period of time. A scenario can be extreme but should be plausible.

Reverse stress testing: Reverse stress testing is a risk assessment technique that works backwards from an adverse outcome for the pension plan and seeks to identify, and aids understanding of, the full range of scenarios and series of events which could have caused that outcome.

Stochastic modelling: Stochastic modelling is a more sophisticated projection modelling approach which starts from the basis that future market conditions (e.g., investment returns, interest rates, and inflation) are subject to a range of future uncertainties. It involves the modelling of many future potential outcomes (typically 1,000 or more) to produce a range of possible outcomes for the plan. It can be used to consider the risks involved in adopting complex investment strategies, or in situations where the risks facing a plan are significant.

As well as financial risk assessment tools, plan administrators should establish mechanisms to assess, monitor, and manage non-financial risks, such as: risks arising from legislative changes, global crises (e.g., pandemic or war), inadequate information technology, internal processes, and data management. While the tools themselves will vary depending on the plan's circumstances and the risks being assessed, plan administrators should take a proactive approach to monitoring all types of risk.

GLOSSARY OF TERMS

Please note that this is not intended to be a complete list of terms but is solely intended to define the terms as used in this document. Please also note that alternative definitions of these terms are possible.

accrued benefits (also known as earned benefits or earned pension) – the amount of accumulated pension benefits that are credited to a plan member based on their length of service, earnings, etc., up to a given date.

actuary – a professional responsible for, among other things, performing valuations of the assets and liabilities of pension plans and calculating the costs of providing pension benefits. In Canada, a pension plan's actuary is typically a Fellow of the Canadian Institute of Actuaries (CIA).

administration – the oversight, management, and operations of the pension plan.

alternative investments – investments in private assets, including real estate, infrastructure, and private equity.

asset – in relation to pension plans, this is anything of monetary value that is owned by the pension plan. This includes cash, investments, property, etc.

beneficiary (or plan beneficiary) – a person who is receiving, or is entitled to receive, a benefit under a pension plan.

controls – arrangements, procedures, or systems, put in place by the plan administrator with the intent of managing a plan's exposure to risk.

cyber risk – the risk of financial loss, operational disruption or reputational damage from the unauthorized access, malicious and non-malicious use, failure, disclosure, disruption, modification, or destruction of information technology systems or the data contained therein.

defined benefit (DB) plan – a pension plan that defines the ultimate pension benefit to be provided in accordance with a formula, usually based on years of service, earnings, on a flat rate, etc.

defined contribution (DC) plan (or money purchase plan) – a pension plan that defines the amount of contributions (including required member contributions, if any) to the pension plan. The member's pension benefits are based on contributions from the member and employer, plus investment income on these contributions. At retirement, the amount of pension that can be bought is based on the accumulated contributions and investment return in the member's account.

emerging risk – a risk which may develop or which may already exist, that is difficult to quantify and may have a high loss potential.

hybrid plan – a pension plan that has both defined benefit and defined contribution provisions.

leverage – leverage exists when any technique or strategy is used to increase a pension plan's economic exposure to investment assets beyond what it could achieve by simply investing its capital (or net assets) in securities or other financial assets.

material risk – Any threat or uncertainty that could significantly impact the stability or financial health of the pension plan.

plan administrator – the individual, group, body, or entity that is responsible for the oversight, management, and operations of the pension plan and pension fund. In some jurisdictions, the plan administrator can also be the plan sponsor.

plan member(s) or member(s) – all current and former employees, including retired employees, entitled to benefits under the pension plan.

plan sponsor – the individual or entity that is responsible for determining the design of the pension plan, setting the benefit structure for various classes of members, and establishing, amending, or terminating the pension plan. This can be the employer or an organization (i.e., employer union) sponsoring the plan. In some jurisdictions, the plan sponsor can also be the plan administrator.

pooled registered pension plan (PRPP) – is a type of pension plan similar to a defined contribution plan; however, employer contributions are not mandatory. A PRPP uses an independent provider, such as a financial institution, to pool contributions together to achieve lower costs in relation to investment management and plan administration.

reverse stress testing – is a risk assessment technique which works backwards from an adverse outcome for the pension plan and seeks to identify, and aids understanding of, the full range of scenarios and series of events which could have caused that outcome.

risk appetite – the amount and type of risk that the plan sponsor is willing to take to meet the plan’s stated objectives (i.e., deliver on promised benefits at an acceptable cost).

risk appetite statement – a document that clearly defines the amount and type of risk that the plan administrator is willing to take to meet the plan’s stated objectives and what the likely responses will be.

risk limits –thresholds that should not be exceeded based on the plan’s risk appetite statement.

risk tolerance – the willingness of an organization to accept or reject a given level of residual risk. Risk tolerance may differ across the organization, based on operating environment, stakeholders, etc., but must be clearly understood by the individuals making risk-related decisions on a given issue.

statement of investment policies and procedures (SIP&P) – a document that contains information about investment policies and procedures in respect of a plan's portfolio of investments and loans. In Quebec, this is referred to as the **investment policy**.

sensitivity analysis – involves identifying variables that affect the finances of the plan or sponsor, changing the values for those variables, and seeing what effect this has on the plan objectives. This helps identify which variables are most important (e.g., interest rates, inflation, equity returns).

sensitivity limits – risk limits that express a pension plan's investment risk appetite in terms of the maximum impact to the plan that the plan administrator is willing to accept under a specific scenario. Sensitivity refers to the impacts to the plan, such as to its investment returns, solvency ratio, minimum funding requirements, and liquidity needs that result from an exogenous shock.

scenario analysis – evaluates the impact of specified scenarios that simulate a specific event considered to be unlikely but plausible.

scenario testing – involves changing the values of several variables simultaneously at a single point in time, in a way that is self-consistent and reflects a chosen economic scenario.

scenario projections – while sensitivity analysis and scenario testing consider the effect of an immediate change in conditions, scenario projections help understand how the plan's finances may evolve in future years. Projection models vary in points of detail, and some can be quite complex.

stress testing – involves performing a scenario projection under a scenario of significantly adverse conditions for the plan, which may be the result of several risk factors materializing, or a severe occurrence of just one risk factor, over a period of time. The scenario would be considered extreme, but plausible.

target benefit (TB) plan – a target benefit plan, also known as a target pension arrangement, is a plan where the contributions are fixed, and the benefits can fluctuate based on the financial performance of the plan. TB plans are typically funded on a going-concern basis.

value-at-risk (VaR) – the maximum loss that could occur with a specified probability over a given time horizon.

wind up – the termination or discontinuation of all (full wind up) or part (partial wind up) of a pension plan, usually at the decision of the employer. This often results from bankruptcy, corporate restructuring, or downsizing.