Guideline No. TBD

Pension Plan Risk Management

Final Draft: As of May 24, 2023

Table of Contents

SECTION 1: INTRODUCTION

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 appropriately.

The primary purpose of a ***pension plan*** is to provide lifetime retirement income to the plan beneficiaries. When administering 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, based on consultation from the industry, determined it appropriate to define the elements of a risk management framework and articulate an approach to identifying, evaluating, managing and monitoring material risks. The risk management principles outlined in this Guideline are overarching principles. 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, see Guideline No. 7 (Pension Plan Funding)).

*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 guidelines.

SECTION 2: SCOPE

Key Takeaways from this Guideline

- create a risk management framework to identify, evaluate, manage and monitor material risks.
- carry out a detailed analysis of your risk management framework regularly.
- the design of each plan's risk management structures and practices will vary based on the plan's characteristics and circumstances, and the risks being assumed.

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

Once a pension plan is established, the plan must be administered, and its assets invested, with the skill, care and diligence required by the standard of care as prescribed under the governing pension legislation for the plan. The establishment 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 request to review the risk management framework prepared by plan administrators on a periodic basis to ensure the pension plan administrator is fulfilling its fiduciary duty.

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, size and the complexity of its administration and investment strategies, the size of the plan membership and plan assets. It is acknowledged that the method of implementing some of the concepts established in this Guideline may differ from one pension plan to another. Plan administrators are encouraged to adapt their risk management practices reflecting their plan's specific circumstances and the risks being assumed.

When designing a risk management framework, plan administrators should take into account 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 may want to consider the separation of duties between those responsible for carrying out operational activities (for example, investment and ***administration***) and those responsible for oversight activities (for example, development of risk management policies and procedures and ensuring that the plan's ***risk tolerances***, limits and controls, timeliness of reporting and escalation are adhered to). This concept, known as independent risk oversight, 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 more complex risk landscape. A systematic approach can help plans to effectively identify and manage their risk exposures.

Risk management is the process of:

- establishing sound governance and oversight that is commensurate with the pension plan's complexity and size;
- establishing processes and methodologies for identifying, evaluating, managing and monitoring material 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 that "*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 in the following areas:

- the way the plan is governed, managed, and administered (including the use of third parties, strategic, reputational and compliance risks);
- the way the plan assets are invested;
- the way the plan's liquidity, funding, and / or benefit adequacy is managed; and
- the way the plan communicates with members.

To be effective, risk management should take into account the long-term nature of pension obligations, but also take into account risks arising over the short term. While risk management is an important consideration for plan administrators in fulfilling their 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, the plan sponsor should consider, based on the current funding and investment strategy, the range of future plan funding contributions and its ability to withstand the variability 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 the ability of the sponsor to continue to fund the plan and discharge its corporate fiduciary duty[1].

Plan Sponsor

For this Guideline, a ***plan sponsor*** is 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.

A plan administrator should consider that:

(i) Plan sponsors may have different stakeholders than the plan administrators (e.g., shareholders)

(ii) Plan administrators and plan sponsors need to work together to identify and manage risks to achieve the shared goal of offering a pension plan; and

(iii) At times, the plan administrator and plan sponsor may be the same entity. Plan administrators should consider how it will resolve any conflicts that arise by virtue of its role as also being plan sponsor, where the plan administrator and the plan sponsor are the same entity.

(iv) The directors and officers of the corporation are subject to the considerations outlined in the Canada Business Corporations Act, section 122 (1.1).

[1] E.g., section 122 (1.1) of the Canada Business Corporations Act provides: ":When acting with a view to the best interests of the corporation under paragraph (1)(a), the directors and officers of the corporation may consider, but are not limited to, the following factors: (a) the interests of (i) shareholders, (ii) employees, (iii) retirees and pensioners, (iv) creditors, (v) consumers, and (vi) governments; (b) the environment; and (c) the long-term interests of the corporation."

SECTION 4: DEFINING THE RISK APPETITE, TOLERANCE AND CAPACITY

A plan administrator and plan sponsor's ***risk appetite***, ***risk tolerance*** and ***risk capacity*** are important considerations in any risk management process.

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

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

Risk capacity is the extent of risk that a plan administrator and its plan sponsor (or, funding agent) is able to support before breaching constraints. It is the capacity to bear risk. This may include the plan administrator's or plan sponsor's ability to withstand volatility in the plan's funded status, cash contributions or probability of maintaining current benefit levels.

Risk Limits

Risk limits represent thresholds that should not be exceeded based on the plan's risk appetite statement.

Risk limits help to ensure risks are effectively managed and that they align with the plan's risk appetite and risk tolerance. In addition to initiating productive ongoing discussions regarding risk and return, risk limits may lead to adjustments to risk appetite, investment policy or investment strategy.

For example, a plan administrator might delegate risk limits with respect to its exposure to certain investments or strategies associated with higher risk. This might include both qualitative and quantitative parameters for individual risk types.

In order to establish controls of the plan (for example, delegation to an investment manager, a third-party administrator or in-house administrator) and provide a mechanism to monitor and manage the plan through regular reporting, plan administrators should consider:

1. establishing an overall risk appetite, risk tolerance and risk capacity, in the form of a written statement; and
2. incorporating these risk limits into the governance and risk management frameworks for their plans.

Considering how to incorporate risk appetite, risk tolerance and risk capacity into the governance and risk management frameworks is both integral and a prerequisite step to constructing the plan's governance and risk assessment frameworks.

SECTION 5: RISK MANAGEMENT FIVE STEP PROCESS

5.1. Step One: Identify Plan's Objectives

A plan sponsor decides to voluntarily offer a pension plan to their employees. In establishing and designing the plan, the sponsor should identify the objectives of the plan, and ensure the objectives are communicated to the plan administrator. The plan administrator should also identify specific objectives for the plan in relation to fulfilling its fiduciary duty to the plan's beneficiaries.

For example, what are the objectives (i.e., desired outcomes) for members' benefit security (e.g., going-concern, solvency and/or wind-up funded ratio targets), predictability (e.g., replacement income target in a target pension arrangement), and affordability (e.g., level and variability of contribution rates)? Other objectives may be applicable as well, depending on the type of plan.

With defined and documented objectives, the plan administrator may then apply risk management practices to increase the likelihood that the objectives are met.

5.2. Step Two: Identifying Risks

The identification of risks provides an opportunity for plan administrators to consider and record all risks to which the plan may be exposed to. There are a wide range of risks that may be relevant to pension plans, and plan administrators are encouraged to review Appendix A: Risk Table for a sample of possible risks facing a plan. In identifying risks, plan administrators may want to consider information drawn from a number of sources, including but not limited to:

- audit reports;
- actuarial reports;
- service provider contracts;
- complaints;
- relevant court cases and decisions;
- administration and investment reports; and

Principles

Identifying Risk
Plan administrators should:

- have a clear understanding of plan operations.
- regularly consider the nature and extent of internal risks.
- regularly consider the nature and extent of external risks.

Evaluating Risks
Plan administrators should:

- develop a process for evaluating and prioritizing risks.
- consider the impact that risks may or will have on plan operations.
- assess the probability of a risk materializing.

Managing Risk
Plan administrators should:

- ensure controls are sufficient to prevent and detect errors.
- understand that controls reduce, but do not eliminate, risk.

Monitoring Risks
Plan administrators should:

- have procedures in place to regularly monitor the effectiveness of controls.
- ensure controls are kept up to date and capable of mitigating new and emerging risks.

- publications about external emerging factors that are likely to impact the plan investments and administration.

The risks identified may be immediate, such as accuracy of member information, cyber or data security, or less imminent, such as the impact of climate change on plan investments. It is also important to understand that risks may be interrelated, correlated, and/or cumulative. Risk identification should therefore also examine the interaction between different risks and consider their interconnectedness.

Many pension plans record all risks identified in a risk register and review it regularly (such as on an annual basis). 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 in place, or that 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 a sample of a risk register template.

Many larger plans in Canada have established a risk committee to provide a structure and dedicated focus for governance of risk identification, assessment and prioritization.

5.3. Step Three: Evaluating Risks

Having identified risks, plan administrators should develop a process for evaluating and prioritizing risks according to the overall threat that they pose to the plan (i.e., the threat of not meeting the plan's articulated objectives), based on the nature, size, complexity and potential impact on the plan's stakeholders.

One common way of evaluating and prioritizing risks is to evaluate the potential severity of the risk against its probability of occurring by utilising a Heat Map approach. Appendix C sets out a sample heat map.

Risk assessment tools can also be helpful in developing a sophisticated approach to risk management and evaluating material risks. Plan administrators should consider the tools appropriate to their plans. Risk assessment tools can be helpful in developing a sound approach to risk management. Common financial risk assessment tools can be found in Appendix B: Risk Assessment Tools.

The prioritization of risk arising from determining likelihood and potential severity will dictate the extent to which mitigating action needs to 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 will require focused attention as it represents a significant threat to the plan.

Risks that are material to the pension plan should be quantified as much as possible. 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.

5.4. Step Four: Managing Risks

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

Controls are arrangements, procedures or systems, put in place by plan administrators with the intent of managing and measuring a plan's exposure to risk. They are an essential component of the plan governance and help to ensure the protection of member benefits. The purpose of controls is to prevent, detect and mitigate errors, irregularities, and fraud. Controls may take many forms, including but not limited to:

- financial policies (investment policy, funding policy, etc.);
- reviews, audits 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 obligation and standard of care. The controls that the plan administrator puts in place should be suitable and proportionate to the scope of the risk. Plan administrators should measure the effectiveness of their controls. Failure to implement effective controls with respect to a known material risk may constitute a breach of the administrator's fiduciary duty.

Once appropriate controls are in place, the plan administrator should then assess based on their risk limits whether to: accept the remaining (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 (especially those which impact across more than one area), with a particular

emphasis on contingency planning. The same process can also help to identify when opportunities arise to reduce plan risk.

No two risks are the same and plan administrators will need to 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 after it materializes. Of course, cost may not be the only consideration when deciding on controls.

Any risk management framework should give the plan administrator reasonable assurance that plan operations are performed properly, including areas with respect to any delegated authority. 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.

Appropriate accountability for the management of a pension plan's operational risks helps to ensure that plan administrators meet their fiduciary and other responsibilities, including the requirement that pension assets are invested prudently. The three lines of defense structure set out in Appendix E: Independent Risk Management and Three Lines of Defense Model is an example of how a plan could set up its risk management governance. It is not appropriate for every size or type of plan, but plan administrators should still consider some form of independent review of the adequacy of the risk management framework put in place.

Example: Risks and Controls for Smaller Plan Relying on third-party Administrators

It is not uncommon for many services to be provided from one or more third-parties. These may include:

- maintenance of books and records;
- calculation of benefits;
- reconciliation of investment holdings; and
- provision of reports for plan administrator meetings.

Where this is the case, plan administrators need to ensure proper oversight in accordance with the standard of care. Plan administrators should ensure that key controls are in place for services which may include peer review of calculations and reconciliations, as well as clear mandates for banking and investment (e.g., authorization procedures) and clear delegations with respect to risk limits and reporting of breaches.

5.5. Step Five: Monitoring Risks

Once plan administrators are confident risk controls have been effectively designed and implemented, they should ensure that they continue to operate effectively. This ongoing monitoring and review process is a key component of managing risk and will ensure that controls continue to be effective.

In performing ongoing monitoring, plan administrators may want to consider information drawn from several available sources, such as audit reports, member surveys, valuation reports, and administration and investment reports.

In summary, risk management is 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 process itself should also be evaluated to ensure its continued effectiveness. Plan administrators are best positioned to determine the appropriate interval for evaluation.

The Big Picture – Asking the Right Questions

Throughout the steps of risk management outlined above, plan administrators should consider the following questions when thinking about the risks identified and their interrelationships:

- what are the key material risks the plan is exposed to, taking account of their potential severity and likelihood?
- how do these material risks impact on the plan separately and together in qualitative and quantitative terms?
- what does this analysis reveal about the totality of the risks that the plan is exposed to?
- have all risks been managed within the risk appetite and is the appetite still appropriate for the plan?
- what risk mitigation measures are available?
- what is the process for reporting breaches?
- what is the process for identifying emerging risks and opportunities?

SECTION 6: SPECIAL CONSIDERATIONS ON SPECIFIC TOPICS

Some of the concepts in this chapter may not be applicable or feasible for all pension plans. Plan administrators are encouraged to adapt their risk management practices reflecting their plan's specific circumstances and the risks being assumed.

Third-Party (Outsourcing) Risk (See Section 6.1)

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, audits, etc.) including to perform specific tasks or to supplement the skills and knowledge of the plan administrator.

This section is relevant to all plan administrators to incorporate the management and monitoring of third-party risk into the plan's governance and risk management framework.

Cyber Security (See Section 6.2)

As pension plans increasingly rely on technology, there is an increasing need to address cyber risk in order to support plan administrators in keeping plan assets safe and protecting the information rights and interests of the plan beneficiaries.

This section is relevant to all plan administrators to integrate cyber risk into the plan's governance and risk management frameworks.

Environmental, Social, Governance Issues (See Section 6.3)

Environmental, Social, Governance (ESG) includes qualitative and quantitative information. ESG information can be relevant to performing a fulsome analysis of risks and opportunities for pension plans. Plan administrators will take different approaches for meeting their standard of care in whether and how they incorporate ESG information into their risk management and disclosure practices.

This section is relevant to all plan administrators in reviewing ESG information to determine which risks and opportunities may affect their plan.

Use of Leverage (See Section 6.4)

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. 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.

This section is to assist plan administrators in establishing policies and procedures to identify and manage risks associated with the use of leverage.

Target Pension Arrangements (See Section 6.5)

A target benefit plan, or more generally, a target pension arrangement ("TPA") is a plan where the contributions are fixed, and the benefits can fluctuate based on the financial performance of the plan. TPAs are typically funded on a going concern basis.

This section is to assist plan administrators in managing risks specific to TPAs, and is focused on three key areas: funding, plan governance and communications.

Investment Risk Governance (See Section 6.6)

Pension standards legislation in Canada requires that the plan 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 shall employ the knowledge or skill that they possess or ought to possess by reason of their profession or business.

This section is to assist plan administrators in meeting their fiduciary and other responsibilities, including the requirement that pension assets are invested prudently.

Considerations for Defined Contribution Pension Plan

The following sections may not be applicable to ***Defined Contribution*** pension plans, including

- 6.5 Target Pension Arrangements, and
- 6.6 Investment Risk Governance.

6.1 Third-Party (Outsourcing) Risk

6.1.1 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, audits, etc.) including to perform specific tasks or to supplement the skills and knowledge of the plan administrator.[2] In the context of a pension plan, typical third-party services include, among other things:

- outsourced activities, functions and services; and
- the use of independent professionals (e.g., lawyers, accountants, third-party pension administrators, actuaries, and investment consultants).

It is important that plan administrators understand that, while the services and responsibilities may be delegated to third-party service providers, the plan administrator 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 6.2.4 (Considerations for Managing Third-party Cyber Risks) for managing third-party cyber risks.

[2] As established in CAPSA Guideline No. 4, 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.

6.1.2 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.

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 people, inadequate or failed processes and systems, or from external events (e.g., cyber incidents); and
- loss of data by the third-party.

6.1.3 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 ensure third-party service providers are in compliance with the plan administrator's overall governance framework and all regulatory requirements. Steps need to be taken by plan administrators to ensure that third-party responsibilities are clearly defined and documented, subject to oversight. This is a risk that all plan administrators and their agents need to be aware of and actively monitor and manage.

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, to ensure appropriate controls are in place to allow the plan administrator to manage the risk. In integrating third-party risk into the plan's governance and risk management frameworks, plan administrators should consider the questions presented in the box below.

Key Considerations on 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 taken into account):

- does the plan administrator understand that it 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, in order to verify the reasonableness of the advice being received?
- is due diligence undertaken prior to entering contracts or other forms of arrangement (e.g., 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 as to ensure 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 on-going basis, whenever there are material changes to the third-party arrangement?
- are third-party arrangements supported by a written contract or other agreement (e.g., service level agreement) that sets out the rights and responsibilities of each party?
- does the plan 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 rate?

As for any other risk, appropriate controls vary depending on the nature, potential impact, and likelihood of the risk at issue. The basic process of risk identification, prioritization, management, and monitoring described in section 5 of this guideline should be followed for all risks, including third-party risk.

6.2 Cyber Security

6.2.1 Background

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

Plan administrators and their third-party service providers control large 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 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 with the care, diligence and skill required of a fiduciary. Steps therefore need to 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 need to 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.

6.2.2 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).

6.2.3 Integrating Cyber Risk Management

To effectively integrate cyber risk management, plan administrators should consider some of the characteristics that make managing cyber risk challenging. This includes the evolving nature of technology, cyber practices, and data standards, the need for specialized technological expertise and training, as well as 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. It should be noted that as cyber risk continues to evolve quickly and, as our understanding and technology evolves, so do the relevant descriptors.

Plan administrators should recognize cyber risk 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. The basic process of risk identification, prioritization, management, and monitoring described in Section 5 of this guideline should be followed for cyber risk, as it should be for all risks.

Key Considerations for Integrating Cyber Risk

In integrating cyber risk into the plan's governance and risk management frameworks, plan administrators 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 ensure that cyber risk is well understood and managed?
- has the plan administrator identified its critical technology assets (e.g., software or hardware), 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?

6.2.4 Considerations for Managing Third-party Cyber Risks

Plan administrators can delegate the retention of large amounts of financial assets, personal and confidential data to third-party service providers. This can make third-party service providers an attractive target for cyber-attacks and exposes the plan to cyber risk.

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

Plan administrators have a duty to ensure that all third-party service providers have implemented sufficient controls to protect plan beneficiary data and plan assets.

Key Considerations for Third-Party Service Providers (this list is not exhaustive and a plan's specific situation should be taken into account)**:**

- cybersecurity posture and cybersecurity capabilities;
- incident management capabilities;
- information technology risks and controls;
- privacy risk management protocols;
- business continuity processes and standards;
- information technology risks and controls;
- certifications and seals of compliance with applicable standards;
- process of how and when the plan administrator would be informed of an incident at the third-party (and applicable subcontractors), its impact on plan beneficiaries and assets, and the frequency of updates throughout the incident;
- process to provide updates on cyber risks and guidance to relevant parties; and
- existence and extent of cyber insurance coverage in place at the third-party service provider.

6.2.5 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, but also to recover when an incident takes place. To ensure effective management of an incident, plan administrators should work with all relevant parties (including in-house functions, third-party service providers and employers) to determine:

- how cyber incidents will be detected;
- how the plan will recover from the incident and restore normal operations (see Resiliency Plans); and
- what disclosures should be made, and to whom, with respect to any incident (see Incident Reporting).

6.2.6 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 the 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 the plan's size; the nature, scope and complexity of its operations; and risk profile.

6.2.7 Incident Reporting

As it relates to 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 them, to plan beneficiaries, and to other appropriate parties;
- determine whether notification of a cyber incident to other parties is required, whether voluntary or as prescribed by any legislation, and should ensure reporting complies with any prescribed timelines;
- inform plan beneficiaries about any cyber incident that has an impact on their benefits, financial or personal interests; and
- ensure that the measures being taken to mitigate the impact of these incidents are communicated to affected plan beneficiaries.

6.2.8 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 be regularly updated on cyber risks, incidents, and controls; 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 Takeaways 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 to ensure appropriate controls are 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 ensure that they 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.

6.3 Environmental, Social, Governance (ESG)

6.3.1 Background

ESG information can be relevant to performing a fulsome analysis of risks and opportunities for pension plans.[3]

Examples of ESG issues that can have economic significance include:

- environmental: climate change, biodiversity loss, pollution, deforestation, flooding and wildfires;
- social: diversity, equity and inclusion, Indigenous rights, employee safety and fair wages, child labour, forced labour and ethical supply chains; and
- governance: board independence, diversity and expertise, executive compensation, financial controls and risk oversight.

CAPSA recognizes that plan administrators will take different approaches for meeting their standard of care in whether and how they incorporate ESG information into their risk management and disclosure practices. Differences in plan circumstances (e.g., type, size and extent of reliance on external asset managers) and investment beliefs affect the kinds and range of decisions to be made by plan administrators. They can also affect how plan administrators view the relevance and materiality of ESG information to those decisions. Cost-efficiency is another relevant consideration; risk-adjusted returns are prudently assessed on a net-of-fees basis. [4]

[3] While this guideline is focused on risk, ESG information can have relevance for identifying not only risks but also opportunities for new investment.

[4] For example, in the context of passive investments, plan administrators may decide these strategies offer competitive investment management costs and align with investment beliefs about the efficiency of public markets to account for material information, including ESG information.

6.3.2 What does fiduciary duty mean in the context of ESG?

When administering 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.[5]

Principle 1:

Pension plan administrators (either directly or through their delegates) should consider whether and how ESG information may be relevant to the investment performance of their funds and take appropriate action based on their determination.

Plan administrators (either directly or through their delegates) should consider whether and how ESG information may be relevant to their pension plans and take appropriate action based on what they determine. 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 performance could be a breach of fiduciary duty.

Plan administrators may determine it is consistent with their fiduciary duty to use ESG information, including for ethical or social impact purposes, as a deciding factor or tiebreaker between otherwise economically equivalent investment options (that is, options that provide equivalent expected risk-adjusted returns). Such use may also arise in the context of stewardship activities such as engagement and proxy voting. Plan administrators should monitor to ensure that any such use of ESG information remains consistent with their fiduciary duty.

In the context of 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 factors as well as "ESG-related funds". Plan administrators should monitor to ensure that the inclusion of such funds remains consistent with their fiduciary duty.[6]

[5] 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*.

[6] An "ESG-related fund" is a fund whose investment objectives reference ESG factors 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).

6.3.3 Implementing ESG Factors in Plan Activities

Plan administrators, as part of their standard of care, should ensure that their plan governance, risk management and investment decision-making practices are designed to identify and respond to material ESG risks and opportunities in a manner appropriate for their plan circumstances and investment beliefs. A review should be conducted at least annually, or whenever there is a material change in the risks facing the plan or governance processes.

The range of issues brought to light by ESG factors are constantly evolving as are the methods and procedures for incorporating ESG information into governance, risk management and investment decision-making practices. Accordingly, practices should be adaptive, responsive and regularly reviewed to assess emerging gaps, risks and opportunities.

Principle 2:

Plan administrators, as part of their standard of care, should ensure that their plan governance, risk management and investment decision-making practices are designed to identify and respond to material ESG risks and opportunities in a manner appropriate for their plan circumstances and investment beliefs. A review should be conducted at least annually, or whenever there is a material change in the risks facing the plan or governance processes.

Governance

CAPSA Guideline No. 4 (Pension Plan Governance) sets out the general expectations of CAPSA with respect to plan governance. With respect to ESG considerations specifically, the plan administrator should ensure that processes are in place to:

- assign responsibility for considering the relevance of ESG information and ensure that materially relevant ESG considerations are included within the plan's risk management framework;
- keep pace with developments in the market regarding ESG practices as well as changes in legislation and regulatory policy; and
- as appropriate for the plan's use of ESG information, assess the ESG skills and experience of the plan administrator and obtain third-party expertise as needed to meet the plan administrator's standard of care.

Third-party expertise can include:

- investment advisors, actuaries 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.

Plan administrators may find it beneficial to develop, and record in written policies, a set of investment beliefs about ESG factors and their application to investment performance. Such beliefs can facilitate better understanding within the administrator and inform governance, risk management and investment decision-making. 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 stewardship) or as a stand-alone document.

6.3.4 Risk Identification and Assessment

Risks identified by ESG factors should not be considered separately but together with other types of risk that are incorporated within a plan's risk profile. However, some of the characteristics of ESG risks complicate the identification, evaluation, prioritization and management of ESG risks, such as

- longer time horizons;
- interrelatedness / correlation with other risks;
- limited or incomplete information, difficulties with quantification;
- modelling complexities; and
- an evolving understanding of their impact and effective management strategies.

As with other risks, plan administrators need to understand the potential materiality of ESG risks to the plan's liabilities[7] and investment portfolio. Periodic analysis and continuing education can help ensure that proper consideration is given to ESG factors in a risk management framework.

Among ESG issues, climate change in particular is considered to pose urgent and material systemic risks[8] to the financial system, which in turn can affect the long-term expected returns of pension plan investments. The physical and transition risks[9] associated with climate change are expected to increase over time; while foreseeable, the magnitude and specific pathways of these risks can be difficult to predict.

In this context, risk models based on historical information are limited. Scenario analysis can be a useful exercise to assess the vulnerabilities of the plan under different plausible risk scenarios, including over different time horizons. Understanding the range of analytical outcomes can lead to a better understanding of potential risks and associated opportunities for the plan's investment strategy and of its funding risks.

[7] It's conceivable that ESG issues, such as climate change and biodiversity, could currently or in the future affect mortality and morbidity rates.
[8] Systemic risks are also considered to be risks that cannot be avoided through diversification.
[9] Physical risks include rising sea levels, increased flooding, extreme heat events and wildfires. Transition risks are those risks associated with transitioning to a more sustainable economy and include inadequate disclosure practices, shifting asset values, changes in consumer preferences and changes in regulations, technology and business practices.

6.3.5. Investment Decision-Making

Investment Strategy

Incorporating ESG risks into investment decision-making – for setting overall portfolio investment strategies and in evaluating individual investments and strategies – can be considered a form of control to manage and mitigate these risks. The implementation of the control however needs to be appropriate for the plan's circumstances and investment beliefs.

Establishing investment limits, targets or standards may be helpful methods practically to manage risk exposures and operationalize ESG investment beliefs. Such limits, targets or standards could, for example, include:

- overall portfolio limits on exposure to green house gas emissions or other ESG risks;
- targets for investment in "green" assets (e.g., green bonds);
- standards of materiality for deciding how ESG factors may affect the investment performance of particular assets or sectors; and
- standards relating to diversity, equity and inclusion, labour and governance practices.

The use of any limits, targets or standards must be consistent with the plan administrator's fiduciary duty and standard of care. Periodic evaluation can help ensure that such tactics are delivering on their intended outcomes and keeping pace with developments in understanding about ESG factors and related practices.

With respect to climate change, developing a plan to understand and manage how the plan's investment strategies are to respond to and address anticipated physical and transition risks, can be a prudent undertaking, depending on the plan's circumstances and investment beliefs, for meeting the plan administrator's standard of care.

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 factors are 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 ESG investment beliefs and risk profile.

Stewardship

Plan administrators undertake stewardship, as appropriate to their plan circumstances and investment beliefs, as a part of prudent investment decision making. Stewardship activities[10] involve a plan administrator seeking to use its position as owner or creditor to influence the activity or behavior of investee companies, asset owners, investment managers, OCIOs or other market participants in ways that reflect the plan administrator's views about ESG risks and opportunities and how to manage them.

Plan administrator's 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.

6.3.6 Disclosure

Stakeholders have an interest in how plans identify and respond to relevant risks and opportunities, and therefore have an interest in being able to clearly understand whether and how ESG information is considered in governance, risk management and investment decision-making practices.

Pension standards legislation in all jurisdictions requires the SIP&P to include a description of factors relevant to investment policies and procedures. Plan administrators should describe whether and how material ESG information is considered or not and make reference to that information in the SIP&P and plan member statements or other sources of plan member information (e.g., websites or fund fact sheets). Disclosure of ESG considerations may be a regulatory requirement in some jurisdictions. Where appropriate, plan administrators should also provide reports on their stewardship activities as well as request companies and asset managers in which they invest to disclose their ESG-related policies.

[10] E.g., voting on corporate resolutions and shareholder proposals, direct exchange with boards and management of investee companies, collaborating with other investors and stakeholders on public policy initiatives and research and industry activities to improve ESG understanding and practices. Stewardship activities also include requesting greater disclosure of ESG policies by investee companies and asset managers to enhance understanding in the market generally about ESG factors.

When ESG information is considered for risk management and investment purposes, best practice suggests the plan administrator make the following minimum disclosures, on an annual basis, in describing how ESG information is considered, and that those be updated on an annual basis:

- 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.

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

Principle 3:

Plan administrators should describe whether and how material ESG information is considered or not and make reference to that information in the SIP&P and plan member statements or other sources of plan member information (e.g., websites or fund fact sheets). Where appropriate, plan administrators should also provide reports on their stewardship activities as well as request companies and asset managers in which they invest to disclose their ESG-related policies.

If a defined contribution plan's investment line-up includes an "ESG-related fund", the plan administrator can demonstrate prudence by describing the rationale for the selection of the ESG-related fund(s) and providing sufficient information for plan members to understand the investment objective and 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.

Plan administrators are encouraged to ensure that they are keeping pace with disclosure developments and industry best practices, such as the Financial Stability Board's Task Force on Climate-related Financial Disclosures (TCFD) and the International Sustainability Standards Board (ISSB).

6.4 Use of Leverage

6.4.1 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.[11]

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.

[11] 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 6.4.3.

6.4.2 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 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.[12]

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.

[12] 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.

6.4.3 Risk Associated with Leverage

This section describes key risks that need to be considered in the context of a plan's use of leverage. The 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[13].

In general, the potential impact of leverage on market risk needs to be considered from both the perspective of 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. 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.[14] 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.

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.

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

[13] 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.

[14] 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.

and its subsidiaries[15]. 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.

6.4.4 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. This includes whether leverage is at the pension plan or fund level or embedded in pooled funds or other investments.

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, measure, monitor and manage exposures and risks;
- assess its capacity and competency to oversee its use of and exposures to leverage; and
- ensuring reporting of the above to those responsible for governance, e.g., senior management and the board of directors/trustees.

- **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.

[15] 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.

6.4.5 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 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 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. These include:

- 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 manager(s) that use leverage are familiar with leverage measurement issues and techniques, including the illustrative metrics;
- that 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.

6.4.6 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 both 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[16] 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 have documented:

- 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 effectively oversee the use of leverage. This includes monitoring and controlling various risks that may arise or be impacted by its use.

6.4.7 Integrating Risk Management

Plan administrators should put in place appropriate systems to effectively 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.

[16] 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.

A plan invests in a pooled fund that employs leverage.

The plan administrator should understand how leverage is being employed by the pooled fund. 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 investment risk metrics should reflect any risks to the pension plan implied by the pooled fund's leverage.[17]

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

6.4.8 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 investment risk generally. They can also help establish parameters and 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***.

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

[17] 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.

6.5 Target Pension Arrangements

6.5.1 Background

A target benefit plan, or more generally, a target pension arrangement ("TPA") is a plan where the contributions are fixed, and the benefits can fluctuate based on the financial performance of the plan. TPAs are typically funded on a going concern basis.

TPAs are generally similar to jointly sponsored or collectively bargained multi-employer pension plans, where a number of employers, usually but not always in the same industry, participate in one pension plan. Contributions are normally fixed through collective bargaining. Note that some jurisdictions currently have legislation that permits single employers to offer TPAs, and plan administrators are encouraged to review the applicable pension legislation to understand the legislative framework pertaining to their plan.

The purpose of this section is to assist plan administrators in managing risks specific to TPAs, and is focused on three key areas: funding, plan governance and communications.

6.5.2 What Types of Risks Should TPA Plan Administrators be Aware of?

Risks that plan administrators should be aware of, and seek to manage and mitigate, include but are not limited to:

- the risk of the plan's target benefit not being achievable due to poor plan design or investment returns failing to meet expectations;
- the risk of plan members not understanding the variable nature of their benefit. In a TPA, there is no risk sharing other than between members of the plan, as the employer contributions are generally fixed and cannot be increased to address a deficit. It is important that plan administrators communicate the concept of benefit variability to plan members;
- the risk of poor plan management/poor plan governance, resulting in:
    - *ad hoc* decisions on benefit adjustments. An example is the risk of "over-benefitting" decisions by pension committees/boards (i.e., the notion of granting benefit improvements when it would be more prudent for the committee/board to not do so) or reducing benefits among classes of members without appropriately considering intergenerational equity factors; and
    - the risk of plan administrators not being appropriately supported with orientation and education policies.

6.5.3 Addressing Risk in Funding, Governance and Communications

Risk associated with TPAs are evolving and will require a dynamic response. Plan administrators should determine strategies to mitigate risks focusing on funding, governance and communications. The list of common tools to address risks associated with funding, governance and communications can be found in Appendix D: Tools for Addressing Target Benefit Risk.

Funding

One of the main considerations in setting the benefit levels of a TPA is whether they can be supported by the contractually required contribution level, which cannot be easily increased.

Plan administrators typically must resort to benefit reductions when faced with a funding shortfall. The variable nature in benefit levels increases the risk of:

- benefit reduction: the plan's targeted benefit levels not being achieved; and
- benefit instability: unacceptable frequency and magnitude of adjustments to benefits.

It is prudent for plan administrators to develop funding and benefit policies, taking into consideration *Special Considerations for Target Pension Arrangements* in CAPSA Guideline No. 7 (Pension Plan Funding Policy).

Governance

On board of trustees' composition, TPAs are unique in that, in many cases, trustees are appointed as a result of a political process (such as an election by a participating group or appointment by an industry association). As such, it is important that plan administrators consider developing policies that ensures the trustees carry out their fiduciary duty.

Communication

It is important that communication policies for TPAs reflect that future or ***accrued*** benefits may be adjusted depending on the financial status of the plan. This concept should be reinforced through various forms of communication, including member presentations and educational sessions, plan booklets and member statements.

Plan administrators are recommended to regularly review their member communications for clarity and consider conducting member feedback sessions to gauge the effectiveness of member communications.

6.6 Investment Risk Governance

6.6.1 Background

Pension standards legislation in Canada requires that the plan 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 shall 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 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.

6.6.2 Considerations for plan Administrators with less sophisticated 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 (for example those that rely on third-party investment managers), the following may constitute an appropriately robust risk management governance structure:

- implementing more frequent governance self-assessments;[18]
- separating oversight of the operational and risk management functions 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.

Accountability for any risk management functions delegated to third-party service providers rests with the plan administrator. 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.

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

6.6.3 Investment Risk Management Practices

Portfolio Limits

Most 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 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. In order 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 policy limit breach does not necessarily require that action be taken to rebalance the portfolio, however repeated breaches should cause the plan administrator to determine whether changes to the risk appetite statement and SIP&P are required.

Risk-Based Sensitivity Limits

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, monitor and periodically review risk-based sensitivity limits. The limits should be linked to the plan's risk appetite and address all material risk exposures.

Operation of Sensitivity Limits

The risk management function should establish appropriate limits based on historical sensitivities to material risk factors consistent with the plan's overall risk appetite. It 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 and/or investment strategy as appropriate following outsized shocks.

Value-at-risk (VaR) is among the metrics that plan administrators use to quantify 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) and/or to mitigate funding volatility (i.e., management of employer’s contributions). In such cases, risk appetite and/or the sensitivity limit is defined as the maximum decrease (volatility) of the plan’s going-concern or solvency position which the plan administrator is willing to accept.

Implementation Considerations

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.

Breaches 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 (when breaches are significant and/or repeated). If the breach is determined to be transitory in nature and/or the plan remains within its overall portfolio risk appetite, no change to the plan’s risk appetite and 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/or asset liability modelling (ALM) are tools used to identify and manage investment risks, the development of the SIP&P and formulation of 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, etc.) 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. Modelling the impact of changes to key risk factors, ALM serves as a tool to assist the plan administrator to manage asset-liability mismatch risk and align investment strategies with the plan’s risk appetite.

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.

Plan administrators are expected to use stress testing and/or ALM corresponding with 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, the stress testing and ALM assist the plan administrator in discharging its fiduciary duties and fulfilling its obligation to invest pension assets prudently.

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 requires specialized market expertise. Plans 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 for their plans processes and controls that provide for appropriate and independent valuation of alternative assets to ensure these are fairly valued.

Plans 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, plans should perform sufficient due diligence on 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 to obtain an independent interim valuation. As a result, plans 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, including for example, performing interim valuations when required during periods of market volatility (stress events).

6.6.4 Portfolio and Risk Reporting

Plan administrators should establish processes and controls to ensure that they have access to timely and comprehensive information to meet their fiduciary and other responsibilities. Portfolio and risk reporting that provides a full view of the investment portfolio and all material risks enables plan administrators to provide effective oversight and challenge to the plan's investment operations, obtain reasonable assurance that pension assets are invested in accordance with applicable pension standards legislation and plan documents, and that pension assets are being invested prudently and in accordance with the plan's risk appetite.

All plan administrators must possess the capacity to produce portfolio and risk reporting, whether internally or through an outsourcing arrangement.

Scope of portfolio reporting

To provide a full view of the investment portfolio, portfolio reporting should include all asset classes, both on-and off-balance sheet and other economic exposures, including but not limited to the following categories:

- public and private market assets
- leverage, including direct and off-balance sheet sources
- notional exposures for derivatives programs
- unhedged foreign exchange exposures

Disclosure should provide a full look-through, if possible, that reflects the underlying holdings of pooled investment vehicles. It should address portfolio limits, including details of portfolio limit breaches that had occurred during the reporting period and/or an action plan to bring the plan into compliance with the SIP&P.

Key Considerations for Outsourced Reporting Arrangements

Information required to produce portfolio and risk reporting may be gathered by the plan administrator and/or third-party service providers including pension fund custodians, investment managers, investment and/or pension consultants and other third parties. Plan administrators should take steps to ensure that they maintain ongoing access to the data and other information they require to produce regular and ad-hoc portfolio and risk reporting.

Plan administrators should ensure that the plan's governance and risk management frameworks provide for appropriate controls to mitigate risks associated with the integrity of such reporting.

Scope of risk reporting

Investment risk reporting should quantify all material investment risks to which the pension plan is exposed, including but not limited to the following categories:

- market risks (i.e., asset price, interest rates and foreign exchange)
- credit risk (including concentration and counterparty)
- liquidity (including investment operations and benefit payments)
- currency / FX risk
- other investment operational risks

SECTION 7: CONCLUSION

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, it is necessary for all pension plans, regardless of plan type, size or assets, to embrace 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 the objectives laid out for it;
- understanding how risks are interconnected, and could simultaneously impact the plan's outcomes; and
- mitigating risks though appropriate tools and controls

As outlined in the introduction, pension regulators may request to review the risk management framework prepared by plan administrators on a periodic basis to ensure the pension plan is fulfilling its fiduciary obligation and standard of care. This may include:

- the risk management framework to identify, evaluate, manage and monitor risks; 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 reflecting their plan's specific circumstances and the risks being assumed.

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 the going concern or solvency bases. 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	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 which increases the value of liabilities by more than the increase in the value of assets.
Model Risk	The risk associated with not accurately capturing and quantifying the liabilities and assets (and their associated volatilities) in a forecasting/projection model, resulting in inappropriate strategic decisions, such as selecting asset mix.
Inter-generational equity	Risk that different generations of plan members experience different outcomes (pension benefits and/or contribution costs) which are perceived as unfair, as a result of poor plan design, funding or decision-making.
Liability / Pension / Actuarial Risks	
Actuarial Methods and Assumptions	Inappropriate actuarial liability valuation methods and assumptions (e.g., expected return on assets, mortality/ longevity, disability, retirement, termination, inflation) resulting in overestimating, or more problematically, underestimating liabilities. Likewise, inappropriate asset valuation methods (e.g., smoothing methods) that consistently over-estimate asset values could lead to underfunding.
Annuity timing	In a defined benefit or target benefit plan that is de-risking or winding up, the risk that annuities are purchased at a rate that is lower than what the fund assets can cover. In a defined contribution plan, the risk that members do not obtain the best price for annuity products, due to market timing. For example, if a retiree purchases an annuity with their defined contribution account balance during a time with especially low interest rates their dollar-for-dollar buying power will be lower versus other retirees who annuitize at a time with more favourable (higher) interest rates and (lower) pricing.

Longevity	In a defined benefit plan, the risk that members live longer than modeled in the actuarial assumptions, resulting in experience losses and increased funding requirements. In a target benefit plan, the risk that members live longer than modeled in the actuarial assumptions, resulting in benefit reductions and potential inter-generational inequity. In a defined contribution plan, the risk that members outlive their retirement savings (where an annuity is not chosen at retirement).
Investment Risks	
Investment Strategy	In defined benefit or target pension plans, the risk that the investment strategy of the plan is not properly aligned with its fiduciary responsibility, risk appetite and tolerance, and/ or long-term investment/ 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 & long-term investment/ 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 without excessive cost or incurring unacceptable losses. Liquidity risk is most present in mature plans (pension payouts exceeding 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 previously assumed obligations, adversely affecting the plan's investments and/or having a reputational impact on 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 investment performance of the pension fund. Poor 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 investment risk (i.e., 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 meltdowns or other economic catastrophes.
Refinancing Risk	The risk that a plan will incur a financial loss as a result of being unable to replace an existing debt obligation required to maintain its leveraged investment positions. 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	Risk that action or inaction related to Environmental, Social and/or Governance factors may negatively impact the value of an investment asset in the future.
Performance Measurement Risk	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 mis-pricing 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 public market volatility.
Governance Risks	
Governance	Risks related to gaps in the oversight over the plan's operation and management, leading to a breach of fiduciary duty. Gaps can exist in plan administrators not receiving adequate orientation, 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	These are the inherent risks with regard to 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 surrounding environment. These include risks related to demographics, competition, technology, conjuncture, interested parties, infection, and political stability. Strategic risks include the continued viability of a plan as a result of change in the operating environment, including internally driven change such as merger, or the coverage of a new group of participants in the pension plan (such as union vs non-union employees with potentially significantly different characteristics and challenges).
Operational Risks	
Information Technology (IT) and Cybersecurity	IT risk is the risk arising from inadequate information technology and processing in terms of manageability, exclusivity, integrity, infrastructure, controllability and continuity. IT risk also arises from an inadequate IT strategy and policy and from inadequate use of the information technology.

	Cybersecurity risks arise from inadequate or failed or vulnerable IT infrastructure and/or software, inadequate policies or policy compliance gaps, and user errors, resulting in the exposure of personally or organizationally sensitive date, or losses due to disruptions in operations.
Litigation	The risk to the plan administrator of members suing them because of a real or perceived negligence, errors, or broken promises, arising from member communications, administrations, or investments, which can lead to financial and/or reputational costs to the administrator.
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 may consist of 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 member benefits; These risks often arise due to inadequate controls or processes in place for effective administration. Operational risk also includes losses due to external events, such as the risk of fraud and general natural disaster risks (e.g., damage to buildings due to fire or natural disasters, burglary or theft).
Fees / Costs	The risk that the commission or fees charged by the service providers (custodians, investment managers, consultants, third-party administrators, etc.) and paid from plan assets (or, in the case of defined contribution plans, from the members' accounts) are unreasonably high, not market competitive, or not properly recorded, or that costs are incurred due to administrative mistakes, and consequently, erode the plan assets / member account balances in the long term. This risk is magnified once a member has transferred their plan account balance out of the plan, to external retail product/service providers.
Political	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.
Communication	Risk of failing to provide members with education and adequate, understandable communication about their benefit entitlements and/or investment options (in defined contribution plans). Communication is particularly important in a TPA, where the risk of plan members not understanding the variable nature of their benefit can result in legal action and reputational damage for the plan administrator.

Regulatory / Compliance	The likelihood of adverse consequences arising from the failure to comply with all relevant laws and regulations. Risks concerning changes in legislation in the future or risks of misinterpreting the legislation.
Plan Sponsor Risks	
Sponsor Risk	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 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, and/or forcing them to transfer their account balance out of the plan, to external retail product/service providers. 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 of the future (downsizing, slowing growth), compared to the current / past demographic composition of the plan.
Participating employer risk	For a multi-employer plan, the risk that a significant portion of the plan's membership is concentrated in a single employer. The withdrawal of such an employer from the plan could result in significant impact to plan funding, increasing contributions and/or reducing benefits (in at TPA) for the remaining participating employers and members.
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 also typically have very long-time horizons and may develop slowly, but mitigating actions equally take a long time to implement and become effective.

APPENDIX B: RISK ASSESSMENT TOOLS

Risk assessment tools can be helpful in developing a sound approach to risk management. Common financial risk assessment tools include the following:

Sensitivity Analysis: Sensitivity analysis involves identifying variables that affect the finances of the plan, 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).

Scenario testing: 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: 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.

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.

Reverse stress testing: 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.

It is equally important that plan administrators establish mechanisms that assess, monitor and manage non-financial risks, such as: legislative changes, global crises (e.g., pandemic or war), business disruption or Information Technology risks, internal processes, and data management. While the tools themselves will vary depending on the plan's circumstances and the risk, it is necessary that plans take a proactive approach to monitoring all types of risk.

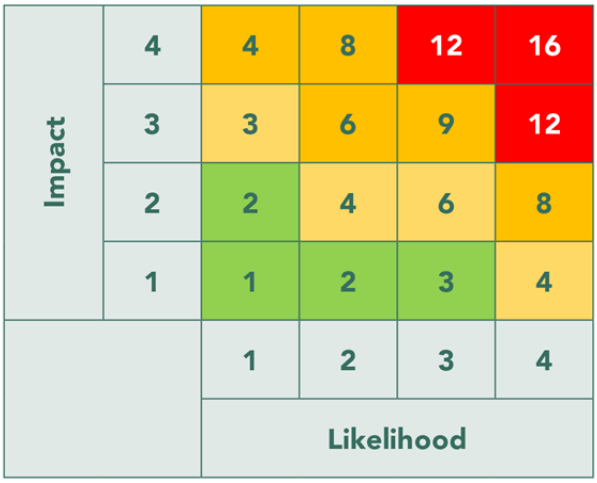
Throughout this process, plan administrators should bear in mind the principles of proportionality, as sophisticated risk assessment tools may be time-consuming and costly, and not necessary if the risks facing the plan are simple and straightforward. Administrators will need to exercise a degree of judgement when considering the costs of implementing these tools and desired degree of sophistication, relative to the benefits.

APPENDIX C: SAMPLE HEAT MAP

Example: Prioritizing Risk Using a 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 1-4 for its probability of occurrence and its severity should be quantified in the context of the plan. They are then multiplied together to see where they are on the heat map (and their level of overall concern). A risk with a likelihood of occurring of 1 and an impact of 1 has a risk rating of green, that is, very low. On the other hand, a risk with an impact of 4 and a likelihood of 4 has a risk rating of red, indicating that the risk should be prioritized.

Example heat map



Example – Cybersecurity: while the plan already has robust cybersecurity protections and training in place, it is recognized that cybersecurity incidents are increasingly common and difficult to prevent. Considering the existing controls in place, the plan administrator rates the probability of a cybersecurity 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 impact on members as high (i.e., 4). The risk rating assigned is therefore twelve, denoting a “Red” level risk rating.

Based on this prioritization exercise, a risk categorized as having high likelihood and high severity will require focused attention as it represents a significant threat to the plan and that further monitoring and controls should be considered.

APPENDIX D: TOOLS FOR ADDRESSING TARGET BENEFIT RISK

Risk associated with TPAs are evolving and will require a dynamic response. In the table below are examples of tools and strategies that can be helpful to address risks associated with funding, governance and communications.

Area of Risk	**Potential Tools**
Funding	**The Provision for Adverse Deviation (PfAD)** is one of the primary tools available to plan administrators to better manage the plan's objectives and ensure adequate funding over the long term. Where applicable, the plan administrator may consider setting different PfADs that apply to actuarial normal cost and going concern liabilities (for example, on a 'plan management' basis in addition to the minimum funding basis). An appropriate policy ladder for benefit changes and restorations, including priority orders of benefit adjustments, may also improve benefit stability, and ensure consistent application of actuarial excess and intergenerational fairness, if this is a desired outcome. It is prudent for plan administrators to develop funding and benefit policies, taking into consideration *Special Considerations for Target Pension Arrangements* in CAPSA Guideline No. 7 (Pension Plan Funding Policy).
Governance	On board of trustees' composition, TPAs are unique in that, in many cases, trustees are appointed as a result of a political process (such as an election by a participating group or appointment by an industry association). As such, it is important that plan administrators consider developing, where feasible and prudent: • a trustee orientation policy, to ensure that new trustees begin their term prepared to carry out their fiduciary duty; • a trustee education policy; and • a trustee succession plan to ensure continuity on the board of trustees.
Communication	Plan administrators should consider the following as they develop a communications policy: • identify the key audience for each piece of communication and tailor each piece of communication to that audience; • maintain regular communication with plan stakeholders; • ensure plan communication materials are in plain language with minimal use of jargon; • keep plan stakeholders informed of significant plan events; and • ensure mutual understanding between plan stakeholders (administrator/trustees, service providers, members) of their roles and responsibilities.

APPENDIX E: INDEPENDENT RISK MANAGEMENT

Independent Risk Management

Accountable for the design and implementation of the plan administrator's risk management framework, the independent risk management function provides objective oversight of the quality and sufficiency of the plan administrator's risk management practices generally, including those performed by operational management. In so doing, it ensures that the risks being taken by the plan administrator are reasonable and within the plan administrator's risk appetite. It provides the plan administrator with objective and timely information and opinions relating to risk that it requires to meet its fiduciary and other obligations, including notification of significant events requiring its attention including repeated breaches of risk-based sensitivity limits (refer to Section 6.6.5) that may signal that the plan's risk appetite has been exceeded.

Separation of the risk management function from operational management is an effective means of maintaining objectivity. Reporting directly to the Board of Directors or Trustees (plan administrator), the plan's administrator's governance structure enables the risk management function to quickly escalate urgent matters. Further reinforcing the independence of the risk management function, the plan administrator and/or employer should implement policies that dissociate compensation of risk management personnel from the financial performance of the pension fund and prevent the involvement of operational management in the performance evaluation and career advancement of risk management personnel. Similarly, risk management personnel should play no role in the making of investment decisions.

Three Lines of Defense Model

Appropriate accountability for the management of a pension plan's operational risks, including investment risks, helps to ensure that plan administrators meet their fiduciary and other responsibilities, including the requirement that pension assets are invested prudently. One way to achieve accountability in the management of a pension plan's risks is to incorporate a three lines of defense structure into the governance and risk management frameworks.

The three lines of defense structure is a means of managing operational risk put in place for federally regulated financial institutions. This structure may also be used to manage risk in pension plans. It offers benefits to pension plans in terms of accountability for the management of its operational risks, including investment risks. It is also consistent with the principle that a pension plan's risk management and operational management functions be separated.

The three lines of defense structure described below is merely an example of how a plan could manage its risk. It may not be appropriate for every size of plan.

Overview of the three lines of defense structure

Operational management constitutes the first of the three lines of defense, the independent risk management function the second with the third being the pension plan or employer's internal audit function. Each of the three lines of defense should be operationally independent of one another.

First line of defense – Operational management

The first line of defense is responsible for the identification and management of the operational risks inherent in the day-to-day operations of the plan including its investment activities, and all of the associated processes and systems. The first line of defense is integral to the risk management framework in that it provides both inputs to (i.e., risk reporting, setting trading limits) and receives outputs from the plan's operational risk management activities (i.e., directions from the independent risk management function).

Second line of defense – Independent risk management function

The role of the second line of defense is to provide objective oversight of the plan's operational risk exposures, taking action as required to ensure that these exposures are consistent with the plan's risk appetite.

Second line activities include the identification of the plan's operational risk exposures, including investment risks. It determines which risks are material, measures and monitors these risks against established portfolio and risk-based sensitivity limits (refer to Section 6.6.5). The second line determines when limit breaches require that corrective action be taken.

The second line of defense is additionally accountable for the development of robust reporting tools that provide the plan administrator with a complete portfolio-wide view of operational risk, including investment risks. It defines the parameters of risk reporting and verifies risk reporting and supporting data provided by the first line to provide the plan administrator with reasonable assurance that it is adequately complete and well-informed.

Third line of defense – Internal audit function

The third line of defense is best placed to observe and review operational risk holistically within the context of the plan's overall governance and risk management frameworks. It provides an objective review and testing of assessment of the effectiveness of operational risk management controls, processes and systems and of the effectiveness of the first- and second-line functions generally.

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 (also known as accrued benefits, earned benefits or earned pension) – the amount of accumulated pension benefits that are credited to a plan member based on his or her 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 person must be a member of the Canadian Institute of Actuaries (CIA) to be recognized as a professional actuary.

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

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 – are arrangements, procedures or systems, put in place by plan administrators with the intent of managing and measuring 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 and/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. A DB plan may be a contributory or non-contributory plan.

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. A DC plan may be a contributory or non-contributory plan.

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

hybrid plan – a combination of defined benefit and defined contribution pension plan.

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.

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 jurisdiction, the plan sponsor can also be the plan administrator.

pension – the monthly, annual or other periodic amounts that start being paid to a member at retirement and that continue for the rest of the member's life.

pooled registered pension plan – is a type of pension plan that is similar to a defined contribution plan; however, employer contributions are not mandatory. A PRPP pools contributions together to achieve lower costs in relation to investment management and plan administration.

registered pension plan – a plan that is organized and administered to provide pensions for employees, and to which an employer is required to make contributions, that is registered in accordance with the **Pension Benefits Act**. It does not include government programs such as the **Canada Pension Plan (CPP)**, the **Quebec Pension Plan (QPP)** or the **Old Age Security (OAS) Program**. Every employer who establishes a pension plan that is subject to the Pension Benefits Act must register the pension plan.

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 administrator is willing to take in order 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 in order to meet the plan's stated objectives and what the likely responses will be.

risk capacity – the extent of risk that a pension plan and its plan sponsor (or, funding agent) is able to support before breaching constraints. It is the capacity to bear risk. This may include the plan's or plan sponsor's ability to withstand volatility in its funded status, cash contributions or probability of maintaining current benefit levels.

risk limits – represent 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.

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).

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 plan – a target benefit plan, or more generally, a target pension arrangement ("TPA") is a plan where the contributions are fixed, and the benefits can fluctuate based on the financial performance of the plan. TPAs 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 (or partial 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.