Office of the Superintendent of Financial Institutions Canada | Bureau du surintendant des institutions financières Canada

# Office of the Superintendent of Financial Institutions

# Internal Audit Report on Regulation Sector:

# Private Pension Plans Division

OSFI BSIF

Canada

# Table of Contents

# 1. Background

**Introduction**

Internal Audit conducts assurance work to determine whether the Office of the Superintendent of Financial Institutions Canada's (OSFI's) risk management, control, and governance processes, as designed and represented by management, are adequate and functioning in a manner to ensure risks are appropriately identified and managed, and to ensure compliance with such requirements as policies, plans, procedures and applicable laws and regulations.

The audit of Private Pension Plans Division (PPPD) was approved by the OSFI Audit Committee and the Superintendent for inclusion in the OSFI 2014 – 2015 Internal Audit Plan.

This report presents the results of that audit based on audit work completed at the end of June 2014.

This report was presented to the OSFI Audit Committee on August 22, 2014 and approved by the Superintendent on September 8, 2014. The Deputy Superintendent, Regulation Sector, and PPPD Senior Management, have reviewed this report and provided their comments.

**Why this audit is important**

Under the OSFI Act, Pension Benefits Standards Act, 1985 (PBSA) and the Pension Benefits Standards Regulations 1985, OSFI, through the Private Pension Plans Division (PPPD), regulates and supervises private pension plans in federally regulated business, works and undertakings, such as banking, telecommunications and inter-provincial transportation. OSFI is also the regulator for pension plans established in respect of employment in the Yukon, the Northwest Territories and Nunavut.

OSFI's mandate strives to protect the rights and interests of beneficiaries of federally regulated private pension plans. The PPPD supports OSFI's mandate by supervising and conducting risk assessments of plans with a view of understanding the risk of loss to members' benefits under its purview, and providing timely and effective intervention and feedback.

*Continued on next page*

# 1. Background, Continued

**Recent events at PPPD**

In May 2012, PPPD upgraded the system supporting its Framework for pension plans. Known as the "Risk Assessment System for Pensions" (RASP), the new system facilitates early identification of issues and integrates OSFI's supervisory tools. Importantly, RASP provides an end-to-end integrated solution to make the risk assessment process more efficient and consistent.

As at December 2012, a new type of pension plan, Pooled Registered Pension Plans (PRPPs) was added to PPPD's purview in accordance with the federal Pooled Registered Pension Plan Act and its associated regulations. OSFI's responsibilities with respect to this new type of pension plan include licensing PRPP administrators, registering PRPPs and providing ongoing supervision. PRPPs can be offered to employers and to self-employed persons under federal jurisdiction. Note that at the time of the audit planning, there were no registered PRPPs under supervision.

**PPPD and risk-based supervision**

The PPPD supervises private pension plans in federally regulated areas of employment and PRPPs in accordance with OSFI's "Risk Assessment Framework for Federally Regulated Private Pension Plans" (Framework). The Framework is risk-based, meaning that the degree of supervisory activity and the level and frequency of OSFI intervention will generally be commensurate with the net risk in a plan.

OSFI's mandate recognizes that the administrator is ultimately responsible for the plan's management, and that a pension plan may experience financial and funding difficulties that may result in a loss of members' benefits. PPPD determines whether the plans meet the minimum funding requirements and are complying with legislative and supervisory requirements. When problems are identified, PPPD promptly advises plan administrators and works with the administrator to ensure the necessary corrective measures are taken to deal with the situation as rapidly as possible.

The PPPD, headed by a Managing Director, has 30 staff and reports to the Deputy Superintendent, Regulation Sector. Of the 30 staff in the group, 13 (one Director, two Managers, and ten Relationship Managers) are on the PPPD Supervision team, tasked to supervise the over 1,200 active pension plans.

Internal Audit last audited PPPD in November 2010, with a focus on approvals management.

# 2. Audit Objective, Scope and Approach

**Audit Objective**

The objective of the audit was to provide reasonable assurance that PPPD's supervisory risk assessment process for pension plans is effective in assessing the possible threat of loss to members' promised benefits. Specifically, Internal Audit examined whether:

1. Management has appropriate processes and controls in place to early-identify pension plans that may have problems meeting minimum funding requirements, complying with the PBSA, or adopting policies or procedures to control and manage risk, and

2. Processes are in place and operating as intended to communicate with plan administrators advising them of material deficiencies and non-compliance issues, and implement interventions to compel administrators to take corrective measures to address deficiencies.

**Audit Scope**

The audit covered PPPD's supervisory work undertaken from April 2013 to April 2014 and included the full PPPD portfolio under supervision during this period.

The audit scope included the following components of PPPD's supervisory process:

- Ongoing monitoring and initial review,
- In-depth review, and
- Intervention.

Recognizing that the supervisory process is a cumulative knowledge process and is continuously evolving, IA reviewed other information relating to events before and/or after the period chosen, as appropriate.

The audit also included an assessment of the sustainability of key systems supporting PPPD's risk assessment process with a focus on systems access and change management to ensure data integrity and reliability of processing.

**Audit Approach**

The audit evaluation criteria, as set out in **Section 4 – Audit Results**, were used for assessing PPPD. These criteria are based on internationally recognized Enterprise Risk Management – Integrated Framework recommended by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).

The approach to conducting the audit included discussions with key personnel, walkthroughs with the PPPD supervision team and examination of supervisory documents and management reports.

# 3. Conclusion

**Statement of Conformance**

The audit was conducted in conformance with the professional internal audit standards of the Institute of Internal Auditors (IIA) and the Government of Canada, as supported by the results of the Quality Assurance and Improvement Program. The evidence was gathered and the procedures used are in compliance with Treasury Board (TB) policies, directives, and both the IIA and TB standards on internal audit.

**Conclusion**

IA is reasonably assured that PPPD, through its supervisory risk assessment process for pension plans, is applying processes and controls to assess the possible threat of loss to members' promised benefits, is effectively communicating with plans and is implementing intervention activity as needed.

PPPD has been faced with operational challenges recently, such as implementation of new systems (for risk assessment, document repository, and regulatory filings) in addition to accommodating a new product (pooled registered pension plans), and the challenging economic environment faced by the plans, PPPD. Nonetheless PPPD has adequately carried out its supervisory activities as intended during the audit scope period. PPPD staff were knowledgeable on the pension plans and worked cohesively as a team, supported by weekly plan update meetings.

As outlined in this Report, there are two areas requiring management's attention;

1. Ensuring that management's in progress review of the Risk Assessment Summary clarifies its purpose and compliance expectations that support an effective contribution to pension plans' ratings. PPPD's current practice to demonstrate support for their assessment of a pension plan's rating differs from the Framework's expectations.
2. Monitoring system access regularly and accurately documenting access permissions to support granting appropriate access.

We encourage management's continuous improvement efforts to update their Supervision Procedures Manual and strengthen their risk assessment process. Important activities initiated recently include the establishment of committees and a formal process to enhance the tiered risk indicators (used to triage potentially higher-risk pensions plans for further supervisory review) and to reassess the fundamentals of their Risk Assessment Summary (a key control in the framework).

We wish to recognize the excellent collaboration of all those involved in the audit. The depth of the review and the ability to focus on what matters would not have been possible without the support received throughout the audit.

_____ _____

Chief Audit Executive, IA Date

# 4. Audit Results

**Audit Evaluation Criteria**

The audit evaluation criteria used for assessing PPPD are based on internationally recognized Enterprise Risk Management - Integrated Framework recommended by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).

| Audit Evaluation Criteria | What We Found |
|---|---|
| **1. Monitoring and Management Reporting** | |
| 1. Ongoing monitoring process is designed and operating as intended to identify and monitor external factors that can negatively impact pension plans, and to assess their impact. | 1. This criterion was satisfactorily demonstrated through IA's review of the external environment monitoring process. |
| 2. Management reporting practices and tools are in place to identify and monitor higher risk pension plans that require more supervisory intensity on a consistent basis. | 2. This criterion was satisfactorily demonstrated through IA's review of the watch-listing process. |
| **2. Process and control Activities** | |
| A. <u>Annual Planning and Ongoing Monitoring of the Plan</u> | |
| 1. Management practices are in place and operating as intended to oversee the planning process and ensure adequate coverage based on risk. | 1. This criterion was satisfactorily demonstrated through IA's review of the annual planning process. |
| 2. Management monitors the plan regularly throughout the year, and where risks to the plan are identified, adjustments are made, documented and communicated appropriately. | 2. This criterion was satisfactorily demonstrated through IA's review of management's ongoing monitoring process. |
| B. <u>Application of the "Risk Assessment Framework for Federally Regulated Private Pension Plans"</u> | |
| 1. Initial review process is designed and operating as intended to early-identify higher-risk plans for more in-depth review and follow-up | 1. This criterion was satisfactorily demonstrated through IA's file review. |
| 2. In-depth reviews are conducted for higher-risk plans in accordance with the Framework; plans' Risk Assessment | 2. This criterion was generally demonstrated through IA's file review. In-depth reviews are conducted for higher-risk plans in |

| Audit Evaluation Criteria | What We Found |
|---|---|
| Summaries (RAS) and resultant Composite Risk Ratings are updated in accordance with PPPD's procedures (e.g. Pensions Supervisory Guidance Notes). | accordance with the Framework. However, for clarity, PPPD should re-evaluate its process to support its assessment of pension plans' Composite Risk Ratings and the intent of the Risk Assessment Summary process (***Recommendation 1***) |
| 3. Intervention activities are undertaken per delegated powers from the Superintendent; rationale supporting intervention activities are documented and communicated to stakeholders (e.g. PPPD management, plan administrator, etc.) per established protocols. | 3. This criterion was satisfactorily demonstrated through IA's file review. |
| C. <u>RASP System (Security and Change Management)</u> | |
| 1. Access to the RASP application is authorized, assigned to ensure appropriate segregation of duties and on a need to know basis (least access principle). | 1. Access to the RASP application is not fully authorized by PPPD. PPPD should approve all access to RASP to ensure appropriate segregation of duties and on a need to know basis (***Recommendation 2***) |
| 2. Access to RASP is reviewed regularly and monitored. | 2. Access to RASP is currently reviewed on an ad-hoc basis. PPPD should implement a process to review system access periodically (***Recommendation 2***) |
| 3. RASP system changes resulting from application updates / new releases and business process changes follow an established change management process. | 3. The 2014-15 filing process will be different due to the implementation of the new Regulatory Return System. Filings reported in RASP with "Errors" in 2013-14 must be corrected immediately to ensure they are validated and loaded into RASP appropriately. (**Recommendation 3**) |
| 4. RASP system underlying business logic, including the Tiered Risk Indicators, is periodically assessed for relevance and any changes arising follow an established change management process. | 4. This criterion was generally demonstrated through IA's review. As part of PPPD's process to review the continued relevance of its Tiered Risk Indicators, it is also formalizing the change management process for modifications to RASP. |

| Audit Evaluation Criteria | What We Found |
|---|---|
| **3. Information and Communication** | |
| 1. PPPD's formal practices and procedures are reviewed periodically to ensure continued relevance, reflecting changes in the environment and supervisory processes. | 1. This criterion was satisfactorily demonstrated through IA's review of policies and procedures. |
| 2. The policies, practices and procedures, and any changes, for the risk assessment process are communicated to staff on a timely basis. | 2. This criterion was satisfactorily demonstrated through IA's interviews with PPPD Supervision staff. |

# 5. Observations and Recommendations

**Observation 1** **Risk Assessment Summary, Plan Rating and the Composite Risk Rating**

Background: The Risk Assessment Summary and the Composite Risk Rating

In accordance with OSFI's "Risk Assessment Framework for Federally Regulated Private Pension Plans" (*Framework*), PPPD's Risk Assessment Summary (*RAS*) is OSFI's assessment of the Overall Net Risk (i.e. inherent risks facing the pension plan and the quality of the plan's risk management), solvency (for defined benefits plans), ongoing performance, and funding.

This assessment culminates into the Composite Risk Rating (*CRR*) which is OSFI's assessment of the overall safety and soundness of the pension plan and the risk that rights and interests of members may not be met. The Direction of Risk (*DoR*) represents the expected trend in the CRR, taking into consideration whether there are significant issues that may not have been resolved or are likely to arise. Action plans are developed to address specific risks and concerns as a result of this assessment.

It is important to note that RASs are not required for all pension plans. Pension plans deemed to have Moderate and Stable CRR and DoR do not require RASs to be completed until circumstances change and indicate some level of risk during the ongoing monitoring and initial review process.

What IA expected

IA expected to see RASs completed for pension plans where indicators of potential for higher risk are triggered, and follow the logic in the RAS to the action plans to address specific risks and concerns highlighted by this assessment.

What IA found

Expected documentation (updated RASs) was either not available or not completed within the timeframe set out in PPPD procedures for some plans. When PPPD identifies material risks or significant concerns on specific pensions plans, any resulting changes to a pension plan's CRR and DoR, watchlist status and staging rating can be updated through a "Plan rating" screen, separate from the RAS. On this screen, the "Plan rating" is accompanied by a short-form analysis and a RAS is not necessarily updated to reflect these changes.

*Continued on next page*

# 5. Observations and Recommendations, Continued

**Observation 1** (continued)

What IA found

Based on IA's discussions with PPPD Relationship Managers, they find the Plan Ratings process to be more dynamic whereas the RAS, although intended to be forward-looking, is a point-in-time assessment that can be quickly outdated. The Supervision team appears to be comfortable making decisions on the pension plans' CRR and DoR without going through the RAS process when significant issues arose and finds that it is more efficient to update the Plan Ratings to highlight supervisory concerns than to complete the full RAS due to operational challenges.

PPPD's current process to assess the CRR and DoR for pension plans is different than the Framework expectations, as the CRR and DoR may be supported by either the RAS or "Plan Ratings" screen. This could lead to inconsistencies and unsystematic assessments across pension plans.

**Recommendation:**

PPPD should re-evaluate its process to support the assessment of pension plans' CRR and DoR. Specifically, it should review the purpose of the RAS and the Plan Ratings screen and how each contributes to its assessment of the pension plan's CRR and DoR (i.e. processes should be fit for purpose).

PPPD should ensure that the documentation of the risks and issues facing a pension plan and the support for the CRR and DoR remains current.

**Management Action Plan:**

We agree with IA's conclusion that PPPD needs to review the manner in which it supports assessments of the CRR and DoR.

In 2013, following recommendations of a committee it established to review workload within the division, PPPD management had identified the issue that IA refers to as meriting attention. As a consequence of this initiative, another committee was convened and is tasked with reviewing PPPD's supervisory practices to ensure that the RAS (including all supervisory processes relating to the RAS) remains fit-for-purpose and meets expectations. The committee will review PPPD's use of the RAS and the Plan Ratings screens to assess and record plans' CRRs and DoRs and will also identify any IM/IT activities that may be required to address business process changes. Recommendations will be finalized by December 2014.

While we anticipate that, where necessary, recommendations will be implemented by September 2015, in accordance with the IM/IT Portfolio

*Continued on next page*

# 5. Observations and Recommendations, Continued

**Observation 1** (continued)

**Management Action Plan** (Continued)**:**

Management audit (2009), any system impacts will be identified to the IM/IT Division in OSFI's annual business planning process and will be subject to review and scheduling through the IM/IT Governance process.

Responsibility: Managing Director, PPPD
Target Date for Completion:

- Changes recommended: December 2014
- Implementation of recommended changes[1]: September 2015

**Observation 2**

**Access to RASP system**

Background: RASP system access

The RASP system is a key system used by the PPPD Supervisory team in its risk assessment process and can trigger supervisory activity and provides input into the fee billing process.

What IA found

IA reviewed access controls for the RASP system to ensure access is authorized, assigned on a need to know basis, and provides for appropriate segregation of duties and found that;

1. PPPD does not have a formal system access review process in place to monitor system access to RASP.
   - Access had not been removed for a few staff that had left OSFI and a couple of staff on leave.
   - Users can be granted access without the approval from PPPD, in particular for non-business users such as information technology (IT) staff. IT staff had access to RASP to support the processing of fee billings, in particular to manage zero balance billings; a process typically assigned to a finance function.

Without approval from the business, and without a regular review of who has what system access, there is a potential for inappropriate access which could impact data availability and integrity.

2. Access is assigned through standard user groups that determine the various system functions and processes the user is able to execute. User groups used in RASP do not match the documented groups, making it difficult to assign the correct access. Furthermore, the documentation of what permissions a user group has is different than the actual permissions granted for many user groups.

*Continued on next page*

[1] RASP related changes subject to review and scheduling through the IM/IT Governance process.

# 5. Observations and Recommendations, Continued

**Observation 2** (Continued)

**Recommendation:**

PPPD should

1. Approve all access to RASP, review the current systems access to RASP and remove inactive and inappropriate accesses that may cause a segregation of duties concern, and implement a process to periodically review system access to RASP going forward,
2. Review the current levels of access allowed for each user group to confirm appropriateness and initiate changes to and/or remove the allowable accesses through the IM/IT Request For Change process as needed, and
3. Review and update its documentation to align with the current levels of accesses in RASP for each user group in the active directory.

**Management Action Plan:**

We recognize the importance of maintaining the integrity and security of the data in PPPD's custody. PPPD has initiated a review of access permissions currently assigned to each category of user within the RASP Active Directory and is in the process of reviewing and, where necessary, removing user access of departed staff and modifying access granted to certain staff. We will monitor individual user access on a monthly basis. We will also implement any necessary changes, consistent with the "least access principle".

A formal process to periodically review the category of RASP access permissions granted to individual users, including protocols pertaining to the granting and timely termination of user access to RASP will be developed, documented and implemented. Further, we will be identifying steps to be implemented to mitigate risks associated with individual users possessing "dual" roles.

PPPD is committed to concluding this project by no later than February 2015.

Responsibility: Managing Director, PPPD
Target Date for Completion:

- Review user roles/definitions and access permissions: September 2014
- Develop and document formal process pertaining to the periodic review, granting and timely termination of user access to RASP: October 2014
- Implement changes to RASP[2]: February 2015

*Continued on next page*

[2] The changes contemplated in its action plan will be incorporated into the scope of a planned system update to RASP, expected to be completed by February 2015.

# 5. Observations and Recommendations, Continued

**Observation 3** **Completeness of regulatory filing in RASP submitted in 2013-14**

Background: Regulatory filings process for 2013-14

In accordance with the Pension Benefits Standards Act, 1985 (PBSA), pension plans are required to file various regulatory filings with OSFI, including the Annual Information Return, Certified Financial Statements, Auditors Reports, Solvency Information Return, Actuarial Valuation Reports and Actuarial Information Summary. With the exception of the Actuarial Valuation Report and Actuarial Information Summary, all of the above filings are received electronically.

PPPD Relationship Managers (RMs) are responsible for ensuring all required filings are received by OSFI. OSFI's Regulatory Data Management (RDM) group, on behalf of PPPD, perform the following tasks related to regulatory filings in 2013-14:

- Entered the filing information into the RASP database,
- Followed-up with plan administrators when issues are detected in the filings. Upon two failed attempts at follow-up, RDM will pass the file onto the PPPD RMs for the next level of follow-up, and
- Monitored late filings and on a monthly basis, produce Late Notification Letters to plan sponsors who have not filed the required filings by the expected due date.

What IA found

There were a number of submitted filings that were rejected by the system, such that the whole filing was withheld awaiting corrections to complete the filing process. Some were from submissions prior to April 1, 2013. Because the corrections were not done, the filings were not loaded into RASP, and therefore these plans would not have been subject to the tiered risk indicator process that facilitates early identification of plan issues. The supervisory process is dependent upon having on a complete set of filings and uses the filings to calculate tiered risk indicators to triage the higher-risk plans.

On IA's enquiry regarding certain filings that had not been corrected, RDM were able to resolve the issue and those filings subsequently passed the validation tests.

Note that the 2014-15 filing process will change because of the implementation of the new Regulatory Reporting System implemented April 2014 such that this control will become obsolete.

*Continued on next page*

# 5. Observations and Recommendations, Continued

**Observation 3** (continued)

**Recommendation:**

All of the filings reported in RASP with "Errors" must be corrected immediately to ensure that any outstanding filing is validated and the filing is loaded into RASP.

PPPD should review these pension plans and confirm that these filings did not impact its assessment of the pension plan's Composite Risk Rating; and that the degree of supervisory activity and the level and frequency of OSFI intervention are appropriate.

**Management Action Plan:**

We concur with IA's assessment of the importance of resolving validation errors.

PPPD has reviewed and taken steps to resolve each of the validation errors referenced in the audit report. The majority of the validation errors identified by IA were found to have been either subsequently addressed or were not valid, although the validation error had not been cleared. These would, for example, include instances where successful validation of a subsequent version of the return had occurred or be due to the filing of regulatory returns that were not required. Of the validation errors identified by IA, relatively few (7) represented genuine validation errors necessitating corrective action. We confirm that failure to promptly resolve these validation errors had no impact upon the risk assessments (e.g. CRR) of the affected plans nor would any interventions have been necessary. As a precautionary measure, PPPD has identified and resolved any additional validation errors that pertained to filings received prior to the period under review by IA. Post-audit monitoring will continue until PPPD is satisfied that the new Regulatory Reporting System has resolved the issue.

Responsibility: Managing Director, PPPD
Target Date for Completion: Completed review of errors report - July 2014

# 6. Management Response

**Overview**

This report has been reviewed by the Managing Director, Private Pension Plans Division and the Deputy Superintendent, Regulation who acknowledge its observations and recommendations.

**Management Response**

We wish to express our appreciation to the audit team for the professional manner in which it has conducted its audit. We are in agreement with the general themes outlined in the audit report.

We are pleased that IA recognizes the effectiveness of PPPD's supervision staff in fulfilling PPPD's mandate. We consider this especially encouraging considering the significant element of change which has recently impacted PPPD's operations, such as the implementation of new systems for risk assessment, document repository, and regulatory filings, in addition to accommodating a new product (pooled registered pension plans), and the challenging economic environment faced by plans. PPPD is committed to continuous improvement in the manner in which it carries out its supervisory work and, in all cases, has initiated steps to ensure that IA's recommendations are addressed in a timely manner.