

REPORT TO: PENSION SUB-COMMITTEE OF THE CITY GOVERNANCE COMMITTEE
& PENSION BOARD – 29 JUNE 2026

REPORT ON: TAYSIDE PENSION FUND INTERNAL AUDIT REPORTS – GDPR, MCCLOUD AND
DATA QUALITY

REPORT BY: EXECUTIVE DIRECTOR OF CORPORATE SERVICES

REPORT NO: 159-2026

1 PURPOSE OF REPORT

To submit the Audit Reports prepared by the Fund's Internal Auditor, PricewaterhouseCoopers (PwC).

2 RECOMMENDATIONS

Members are asked to note the content of the report on the audit exercises undertaken, and to approve the management responses.

3 FINANCIAL IMPLICATIONS

There are no financial implications arising from the agreed recommendations in this report.

4 MAIN TEXT

4.1 Internal Audit Report – GDPR Review (Appendix A)

4.2 The report presents the findings of the recent audit review of GDPR arrangements within the Tayside Pension Fund. The audit examined the adequacy and effectiveness of the Fund's governance, policies, and controls in ensuring compliance with data protection legislation, with a particular focus on data handling, security arrangements, record management, and oversight mechanisms. The objective was to obtain assurance that appropriate processes are in place to manage personal data securely and in line with statutory requirements.

The audit concluded that while key controls are in place and operating in most areas, opportunities exist to strengthen arrangements further. The recommendations set out in the report have been agreed by management, who have provided action plans to address the issues identified within agreed timescales.

4.3 Internal Audit Report – McCloud Review (Appendix B)

The report presents the findings of the McCloud Post-Implementation Review undertaken in respect of Tayside Pension Fund. The review assessed the effectiveness of the arrangements put in place to implement the McCloud remedy, including governance and oversight, data management, calculation processes, member communication, and compliance with relevant legislation and guidance. The objective was to provide assurance that the remedy has been implemented appropriately and that associated risks are being effectively managed.

The review concluded that, while the implementation framework is broadly sound, there are opportunities to strengthen controls and supporting processes in a number of areas. The recommendations detailed in the report have been agreed by management, with action plans in place to address the issues identified within agreed timescales.

4.4 Internal Audit Report – Data Quality (Appendix C)

The purpose of this report is to present the findings of the data quality (data gap) review undertaken in respect of Tayside Pension Fund. The review examined the completeness, accuracy and reliability of

member data held by the Fund, with particular focus on the identification and management of data gaps, controls over data input and maintenance, and compliance with regulatory expectations. The objective was to provide assurance that data is fit for purpose to support benefit administration, statutory reporting and ongoing regulatory requirements.

The review concluded that, although a framework exists to manage data quality, further work is required to address identified data gaps and strengthen supporting controls. The recommendations set out in the report have been agreed by management, with action plans established to deliver improvement within defined timescales.

5 POLICY IMPLICATIONS

This report has been subject to the Pre-IIA Screening Tool and does not make any recommendations for change to strategy, policy, procedures, services or funding and so has not been subject to an Integrated Impact Assessment. An appropriate senior manager has reviewed and agreed with this assessment.

6 CONSULTATIONS

The Chief Executive and Head of Democratic and Legal Services has been consulted on the content of this report and agree with the contents.

7 BACKGROUND PAPERS

None

PAUL THOMSON
EXECUTIVE DIRECTOR OF CORPORATE SERVICES

22 JUNE 2026



Internal audit report 2025/26

GDPR Review

Tayside Pension Fund (TPF)

Final Report



Final Report

PwC

11 June 2026

This page is intentionally left blank

3	Executive Summary
5	Current year findings
14	Appendices
15	Appendix A: Basis of our classifications
17	Appendix B: Terms of reference
19	Appendix C: Limitations and responsibilities

Contents

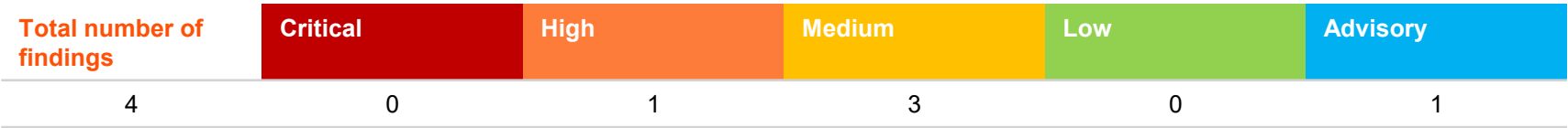
This page is intentionally left blank

Executive Summary

Report classification

High risk

Refer to Appendix A for the basis of classification



Background

Tayside Pension Fund (TPF), administered by Dundee City Council as part of the Local Government Pension Scheme in Scotland, manages the pension arrangements of over 56,900 members across 41 employers. While TPF oversees its own operational activities, it relies on Dundee City Council for wider data protection governance, including policies, breach management and legal support. TPF’s internal data protection function is small, with a single staff member undertaking data protection management responsibilities and escalating matters to the Council’s Data Protection Officer, whose duties are currently being covered by the Council’s legal team. While this audit focuses on TPF, several findings overlap with Dundee City Council where responsibilities and controls fall under the Council’s remit rather than the Fund’s.

The objective of this audit was to provide an independent assessment of TPF’s key data protection risks and to review the design and operation of controls in place to support compliance with UK GDPR requirements, including governance arrangements, oversight provided by Dundee City Council, and the Fund’s handling of core data protection processes (*refer to Appendix B for the detailed terms of reference extract and scope areas*). Please find an overview of our observations aligned to each objective below:

- Governance and Oversight:** Data protection responsibilities currently sit with the IT Systems and Process Analyst, and quarterly reporting on data protection risks is in place, although the information provided is high level.
- Policy Requirements:** The Information Governance Policy provides a high-level framework for data protection, but TPF lacks dedicated procedures for key areas such as breaches and data subject rights.
- Record of Processing Activity (RoPA):** No Article 30-compliant RoPA was available. Management indicated that some processing information was embedded in the privacy notice; however, this is not sufficiently detailed or aligned to UK GDPR requirements (e.g., data categories, retention, recipients, transfers, etc.) .
- Data Subject Access Requests (DSARs):** Data subject rights requests are low in volume and have been completed within statutory timelines, although the DSAR process is not formally documented and relies on local knowledge. Some rights, such as rectification, are effectively managed through the member portal, which helps maintain data accuracy and reduce manual processing.
- Breach Notification Procedures:** A breach reporting and investigation workflow is in place and supported by regular team awareness, with evidence of lessons learned following a recent larger incident. However, there is no written breach procedure specific to TPF. From discussions with management following the recent breach, we understand that communication with affected individuals is carried out, and this approach aligns with ICO expectations
- Staff Training:** Mandatory GDPR training is in place with improving completion rates, although role-specific training and a structured awareness programme do not currently exist, with ongoing awareness instead maintained through informal mechanisms such as team meetings and ad-hoc communications.

Executive Summary

Overall conclusions

The internal audit of Tayside Pension Fund observed a baseline standard of data privacy controls, with evidence that the data protection team focuses its available capacity on areas of greatest regulatory exposure, such as responding to individual rights requests and managing personal data breaches. Core compliance activities, including DSAR handling and breach reporting, are operating effectively in practice, with low volumes of requests processed within statutory timelines and all breaches appropriately escalated to the ICO within required deadlines.

There is, however, a need for more documentation and structure to strengthen TPF's overall control environment. The absence of an Article 30 Record of Processing Activities, the lack of Fund-specific procedures for DSARs and breaches, and insufficient management information restrict TPF's ability to demonstrate accountability and provide consistent oversight of key compliance indicators. Current training and awareness measures, administered through Dundee City Council, provide a baseline understanding but do not extend to annual refreshers, role-based learning or embedding a privacy culture.

Strengthening documentation, governance, reporting structures and role-based capability would support TPF in maturing its data protection framework and enhance its ability to evidence compliance with UK GDPR requirements. TPF has already demonstrated a willingness to engage constructively with improvement actions, and with modest enhancements to processes and oversight, TPF will be well positioned to further embed a strong but proportionate privacy control environment.

Summary of findings:

- **Absence of a Record of Processing Activities (RoPA)** (*High*) - TPF were not aware of a Record of Processing Activities (RoPA) at Dundee City Council and no RoPA was provided, indicating that the Council, as data controller, does not currently demonstrate the Article 30 accountability requirement to maintain a structured and centrally governed record of its personal data processing activities.
- **Opportunity to uplift Data Protection Procedures** (*Medium*) - TPF has an opportunity to uplift its procedures by formally documenting processes for data breaches and data subject rights requests, as current reliance on staff knowledge may create gaps if key individuals leave or new staff join.
- **Training and cultural awareness measures require strengthening** (*Medium*) - TPF currently relies on Dundee City Council's GDPR e-learning module, which is completed every two to three years, and does not provide role-based training or regular privacy awareness activities. As a result, staff may not receive sufficiently frequent or tailored guidance to maintain up-to-date knowledge, strengthen specialist capability or reinforce a strong privacy culture.
- **Insufficient management information** (*Medium*) - Management information reporting within TPF is insufficient, with quarterly updates lacking key performance indicators (KPIs) or key risk indicators (KRIs) needed to track data protection compliance activities such as policy reviews, training completion and DSAR timeliness. In addition, TPF does not have formal data protection governance forums with Dundee City Council, resulting in inconsistent oversight and limited visibility of shared responsibilities and risks.

We also identified the following areas of good practice:

- Data protection risks are reported regularly to the relevant committee, providing ongoing oversight and ensuring that emerging issues are escalated and monitored as part of routine governance.
- Data subject access requests are effectively managed due to consistently low volumes, with all requests logged, tracked and completed within the statutory 30-day timeframe.
- All personal data breaches have been notified to the ICO within the required 72-hour period, with follow-up actions incorporating lessons learned, and communications to affected individuals issued through appropriate channels such as email, post and phone in a manner aligned with ICO expectations.
- Certain data subject rights, such as rectification, are handled directly through the member portal, enhancing data accuracy controls and reducing the need for manual administrative processing.

Findings

1 Absence of a Record of Processing Activities (RoPA)

Operating effectiveness



Finding Rating:
High

Finding

During our review, Tayside reported that they were not aware of whether Dundee City Council maintains a Record of Processing Activities (RoPA). As Dundee City Council is the Data Controller, it is responsible for ensuring that a RoPA exists and is appropriately governed. Based on the information provided and discussions held, no RoPA was provided to demonstrate that a centrally maintained record is in place or accessible to relevant stakeholders, including the Tayside team.

Management noted that some high-level information about personal data processing appears within the Council's external privacy notice. This does not meet the requirements of Article 30 of the UK GDPR, or the expectations set out by the ICO. The accountability principle requires organisations to maintain a detailed internal record of processing activities under their responsibility that can be provided to the regulator on request.

A compliant RoPA must include, for each processing activity, the purpose of the processing, the categories of data subjects and personal data, the categories of recipients including processors and third parties, details of international transfers and associated safeguards, the retention periods that apply and a description of the technical and organisational measures used to protect the data. The ICO expects organisations to maintain this in a structured and standalone format, typically a spreadsheet or software solution, to support transparency and enable oversight of data protection risks.

RoPAs are commonly administered centrally by the Data Protection Officer. However, some organisations adopt a distributed model in which business areas or service lines have Data Champions that maintain their own domain specific entries. For example, Tayside could be asked by Dundee City Council to maintain the RoPA applicable to its processing activities, provided that the Council's DPO retains full visibility and governance oversight of the complete organisational RoPA.

Potential Implication

The absence of a documented and centrally governed Record of Processing Activities (RoPA) at Dundee City Council limits the Council's ability to demonstrate compliance with Article 30 of the UK GDPR. As TPF undertakes processing on behalf of Dundee City Council, the lack of an organisational RoPA also prevents TPF from having clarity on how its processing activities fit into the wider data protection framework. Without a RoPA for TPF to contribute to or reference, there is an increased risk that processing activities are not fully understood, appropriately documented or aligned with the Council's lawful bases, purposes and retention requirements. This creates operational uncertainty for Tayside, increases the risk of inconsistent practices across service areas and may hinder the Council's ability to respond effectively to data subject rights requests, incidents, and regulatory enquiries.

Findings

1

Absence of a Record of Processing Activities (RoPA)

Operating effectiveness

Finding Rating:
High

PwC Recommendations

1. Identify and document all processing activities carried out on behalf of Dundee City Council, ensuring these can be incorporated into the central RoPA once established. The ICO provides a [template](#) designed for this purpose, and following this structured approach will support the creation of a comprehensive RoPA.
2. Once developed, ownership of the RoPA should be formally assigned to an appropriate role, with a clear maintenance process to ensure that it is reviewed and updated regularly, ideally at least annually or whenever business processes or systems change.

Management Actions

The team will perform the following and get them formally approved by senior management:
The Dundee City Council Data Protection Policy 2019 makes reference to the Register of Processing and this has been located. Some further work is planned to refresh and consolidate existing data mapping activity into a fully compliant, centrally maintained RoPA .

Responsible person/title:
Roger Mennie - Head of Legal and Democratic Services

Due Date
31st March 2027

Findings

2 Opportunity to uplift Data Protection Procedures

Operating effectiveness



Finding Rating:
Medium

Finding

Dundee City Council's Information Governance Policy covers data protection requirements at a high level. However, TPF does not have any Fund-specific operational guidance that translates these wider Council requirements into clear internal steps for the team. While the Council's policy references subject access requests and incident management, these references remain generic in nature and do not describe the processes and practical steps followed within TPF itself.

In addition, where TPF relies on legitimate interests as a lawful basis for processing, there is currently no documented Legitimate Interest Assessment (LIA) to demonstrate that the requirements of UK GDPR Article 6(1)(f) have been met. ICO guidance indicates that organisations should evidence the purpose test, the necessity test, and the balancing test to ensure that individuals' rights and freedoms have been appropriately considered. The absence of a formal LIA creates a gap in demonstrating compliance with lawful basis requirements and increases the risk of challenges from data subjects or the regulator.

TPF relies on staff knowledge and experience to manage activities such as data subject access requests, data breach handling, and decisions related to lawful basis assessments, including legitimate interests. Although management confirmed that these processes are well understood within the team, they are not formally documented. This creates an opportunity for TPF to uplift its procedures by documenting these key processes to ensure consistency and operational resilience, as reliance on informal knowledge may lead to gaps if key individuals leave or if new staff join the organisation.

Potential Implication

The absence of written procedures means that TPF may be exposed to operational continuity risks, particularly in situations where key staff are unavailable or where new staff require onboarding. Documented procedures would help ensure clarity on roles, responsibilities, escalation points and statutory timescales, and would support greater consistency in the way rights requests and incidents are handled.

Findings

2

Opportunity to uplift Data Protection Procedures

Operating effectiveness

Finding Rating:
Medium

PwC Recommendations

1.

TPF should develop a set of written internal procedures that set out, how TPF manages DSARs, data breaches, DPIAs and other key data protection activities. In addition, these procedures should be simultaneously reviewed alongside Dundee City Council's Info Gov Policy to ensure alignment and consistency with the Council's overarching framework.
2.

TPF should then assign clear ownership for maintaining the procedures, and ensure the procedures are approved through the appropriate governance channels. TPF should also implement a regular review cycle to ensure the procedures remain accurate and up-to-date.

Management Actions

The team will perform the following and get them formally approved by senior management: While formal documented procedures for subject access requests, breach management and lawful basis assessments are not currently in place, established processes are operating effectively in practice and are supported by appropriate tracking mechanisms. Notwithstanding this, we recognise the benefit of formalising these arrangements to enhance consistency, resilience and auditability, and will take this forward on a proportionate basis.

Responsible person/title:
Roger Mennie - Head of Legal and Democratic Services

Due Date
31st March 2027

Findings

3 Training and cultural awareness measures require strengthening

Operating effectiveness



Finding Rating:
Medium

Finding

Current training arrangements for TPF rely on Dundee City Council's formal GDPR e-learning module, which is completed on a two-to-three-year cycle. While we recognise that responsibility for administering this training sits with the Council rather than the Fund, it is considered good practice for staff who handle personal data to refresh their understanding annually. Refreshed annual content could include revised content or questions banks to ensure training is engaging, relevant and improving employees-based knowledge over time. More frequent training helps ensure that key principles remain current in staff thinking and reduces the risk of outdated knowledge influencing day-to-day decisions.

There is currently no role-based data protection training available for staff who hold enhanced responsibilities. In particular, the Data Protection Lead would benefit from structured development focused on the practical requirements of the role. This may include formalised, role-specific training modules or access to an external qualification to support capability building and ensure ongoing confidence in fulfilling statutory and organisational obligations.

A recommended route for external professional development is the suite of qualifications offered by the International Association of Privacy Professionals (IAPP), which are widely recognised across the industry:

- CIPP/E: Provides a comprehensive understanding of European data protection legislation, including the UK GDPR and associated regulatory frameworks. It is considered the leading foundational qualification for privacy professionals in Europe.
- CIPT: Focuses on the integration of privacy into technology and system development. It supports the practical application of privacy engineering principles and techniques to reduce risk throughout the software and systems development lifecycle.
- CIPM: Designed for professionals responsible for operationalising privacy within business functions such as HR, marketing, finance and customer services. It equips practitioners to establish, manage and monitor a privacy programme, reducing organisational risk arising from inappropriate handling of personal data.

Together, these qualifications provide a structured and credible foundation for developing and sustaining privacy expertise within TPF.

We also noted that TPF does not currently run additional privacy awareness campaigns to reinforce core responsibilities throughout the year. Regular reminders can support a positive privacy culture and reduce the likelihood of human error. Simple interventions such as periodic emails, posters, short awareness messages would help maintain visibility of privacy principles between formal training cycles.

Findings

3 Training and cultural awareness measures require strengthening

Operating effectiveness



Finding Rating:
Medium

Potential Implication

A training programme that is infrequent, generic and not supplemented by ongoing awareness activity risks becoming a tick-box exercise rather than an engaging and meaningful mechanism for building capability. Without annual refresher training, role-specific development or regular prompts that reinforce privacy expectations, staff may not retain the depth of understanding required to manage data protection obligations confidently. This risk increases further where individuals take on data protection responsibilities such as handling rights requests, maintaining records of processing or supporting breach escalation without adequate preparation, heightening the likelihood of procedural errors, inconsistent data handling and gaps in regulatory compliance.

In addition, the regulatory landscape is evolving rapidly, with emerging frameworks such as the EU AI Act, the UK's Data (Use and Access) Act 2025 (DUAA), and the future EU Digital Omnibus set to introduce new or expanded requirements relating to transparency, risk management, accountability and automated decision-making. Without a training programme that is proactively updated to reflect these developments, the Council may be unable to equip staff with the knowledge needed to respond to changing obligations. This increases the risk of policies and operational practices becoming outdated, resulting in non-compliance, misalignment between process and regulatory expectations, and reduced organisational readiness for forthcoming regulatory change.

PwC Recommendations

1. TPF should work with Dundee City Council to explore the feasibility of implementing annual refresher training for all staff who process personal data, ensuring a more consistent and timely reinforcement of GDPR obligations.
2. TPF should also introduce role-based development for individuals with enhanced responsibilities, particularly the Data Protection Lead, which may include more detailed internal training or support to pursue an external accreditation.
3. In addition, TPF should introduce periodic privacy awareness initiatives such as short communications, posters, or scheduled reminders during team meetings. These measures will help ensure that training becomes a more engaging and continuous learning experience, strengthen staff confidence in managing compliance activities, and contribute to a more effective privacy culture across the TPF.

Findings

3

Training and cultural awareness measures require strengthening

Operating effectiveness

Finding Rating:
Medium

Management Actions

The team will perform the following and get them formally approved by senior management: We note the recommendation in relation to annual refresher training. While current training arrangements across the Council operate on a longer cycle, we will consider, in conjunction with relevant services, whether there are proportionate opportunities to enhance awareness through targeted or role-specific interventions. GDPR is discussed as a standing agenda item at the fortnightly team meeting to maintain staff awareness of the importance.

Responsible person/title:
Amanda Smith - Team Leader

Due Date
31st March 2027

Findings

4

Insufficient management information

Operating effectiveness



Finding Rating:
Medium

Finding

The management information currently produced by TPF is limited in scope. Quarterly reporting to senior management is in place; however, the content focuses primarily on high-level matters and does not include structured Key Performance Indicators (KPIs) or Key Risk Indicators (KRIs) that would allow TPF to monitor the effectiveness of its data protection compliance activities over time. Areas such as policy update cycles, training completion rates, Record of Processing Activities maintenance, DPIA completion and review, and the timeliness of data subject rights responses are not routinely captured or presented in management reports. Introducing more defined indicators would support clearer oversight, improved trend analysis, and more informed decision-making (e.g., when allocating resources).

We also observed that TPF does not have formal governance forums in place with Dundee City Council in relation to data protection. Interaction with the Council's Information Governance and Legal teams currently occurs on an informal, as-needed basis, and while these touchpoints are helpful, the absence of a structured forum means that data protection risks and progress on compliance activities are not reviewed through a consistent process. Establishing a defined governance structure with the Council would help ensure clearer accountability, provide greater transparency over shared responsibilities.

Potential Implication

Without structured management information and formal governance arrangements, senior management may not have sufficient visibility of TPF's data protection risks. The lack of regular KPI monitoring limits TPF's ability to identify trends, track improvements or intervene early where performance is declining. Informal governance arrangements may also lead to inconsistency in decision-making and reduce TPF's ability to evidence compliance with the UK GDPR accountability principle.

PwC Recommendations

1. TPF should enhance their current quarterly management information pack to include clear data protection KPIs, covering areas such as policy reviews, training compliance, ROPA updates, DPIA completion and data subject rights performance.
2. TPF should also establish a formal governance forum, supported by a defined agenda, clear responsibilities and appropriate record-keeping, to provide senior management with regular oversight of data protection matters.

Findings

4

Insufficient management information

Operating effectiveness

Finding Rating:
Medium

Management Actions

The team will perform the following and get them formally approved by senior management:
As part of the ongoing structure review, a dedicated role is currently being progressed which will include responsibility for strengthening data protection governance, coordination and oversight across the Tayside Pension Fund which will address the management information recommendation.

Responsible person/title:
Amanda Smith - Team Leader

Due Date
31st March 2027

This page is intentionally left blank

Appendices

This page is intentionally left blank

A) Basis of Classifications (1/2)

Individual finding ratings

Critical



A finding that could have a:

- **Critical** impact on operational performance; or
- **Critical** monetary or financial statement impact; or
- **Critical** breach in laws and regulations that could result in material fines or consequences; or
- **Critical** impact on the reputation or brand of the organisation which could threaten its future viability.

High



A finding that could have a:

- **Significant** impact on operational performance; or
- **Significant** monetary or financial statement impact; or
- **Significant** breach in laws and regulations resulting in significant fines and consequences; or
- **Significant** impact on the reputation or brand of the organisation.

Medium

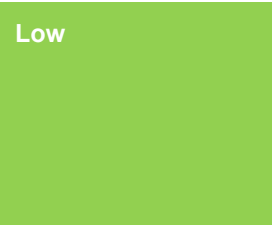
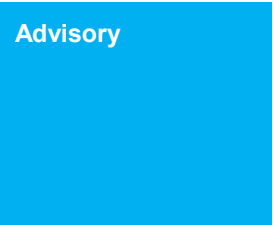


A finding that could have a:

- **Moderate** impact on operational performance; or
- **Moderate** monetary or financial statement impact; or
- **Moderate** breach in laws and regulations resulting in fines and consequences; or
- **Moderate** impact on the reputation or brand of the organisation.

A) Basis of Classifications (2/2)

Individual finding ratings

Low			A finding that could have a: • Minor impact on the organisation's operational performance; or • Minor monetary or financial statement impact; or • Minor breach in laws and regulations with limited consequences; or
Advisory			Minor impact on the reputation of the organisation A finding that does not have a risk impact but has been raised to highlight areas of inefficiencies or good practice.

Report classifications

The report classification is determined by allocating points to each of the findings included in the report.

Findings rating	Points	Report classification		Points
Critical	40 points per finding		Low risk	6 points or less
High	10 points per finding		Medium risk	7 – 15 points
Medium	3 points per finding		High risk	16 – 39 points
Low	1 point per finding		Critical risk	40 points and over

B) Terms of reference extract: Audit scope and approach (1/2)

Scope

Our scope will consist of the following:

Scope Area	Objectives and areas of review	Risks
Governance and Oversight	Governance mechanisms have been defined establishing clear roles and responsibilities and effective reporting arrangements to Senior Management and the Board.	Poor governance can lead to non-compliance, data breaches, and reputational damage.
Policy Requirements	A policy is approved detailing requirements for data collection, processing, storage, and sharing, ensuring alignment with applicable regularity standards i.e., UK GDPR and DPA.	The absence of policy requirements can result in non-compliance, leading to legal penalties, loss of stakeholder trust, and data breaches.
Record of Processing Activity (RoPA)	A system is in place to ensure the record of processing activities is complete, accurate, and regularly maintained, reflecting actual data processing practices.	Inadequate maintenance of processing activities can lead to discrepancies, and diminished trust from data subjects and stakeholders.
Data Subject Access Requests (DSARs)	Procedures are established for the compliant handling of data subject access requests, including identity verification and mechanisms to track and report requests.	Inefficient data access handling can result in compliance failures, legal issues, and a loss of trust.
Breach Notification Procedures	An incident response plan and breach notification procedures are in place ensuring timely communication with relevant parties and the integration of lessons learned.	Inadequate incident response can lead to fines, loss of customer trust, and missed opportunities to prevent future incidents.
Staff Training	A training program is in place that delivers role-specific education to all employees ensuring effective awareness of data privacy practices across the organisation.	Insufficient training can result in a lack of data privacy awareness, leading to non-compliance and increased risk of breaches.

B) Terms of reference extract: Audit scope and approach (2/2)

Limitations of scope

This audit will focus on assessing the processes in place for ensuring there is sufficient oversight of key service providers, specifically the scope is limited to the objectives noted above. We will not perform the following.

- An end to end regulatory compliance assessment.
- Confirm that all artefacts are compliant with regulatory requirements.
- Verify that incidents have been adequately classified.
- Any other area not specifically included within the internal audit scope section.

Any observations we may report are limited to those identified through the course of our work and are not intended to represent an exhaustive list of all potential issues or considerations. Our work is not designed to ensure compliance with all laws and regulations. Fraud, error, or non compliance with laws and regulations may occur and not be detected. Furthermore, the scope of our work does not constitute assurance over compliance with any laws and regulations.

Audit approach

Our audit approach is as follows:

- Obtain an understanding of the in-scope areas via discussions with key personnel, review of documentation.
- Identify the key risks of the process.
- Evaluate the design of the controls in place to address the key risks.
- Test the operating effectiveness of the key controls.

C) Limitations and responsibilities

Limitations inherent to the internal auditor's work

We have undertaken this review subject to the limitations outlined below:

Internal control

Internal control systems, no matter how well designed and operated, are affected by inherent limitations. These include the possibility of poor judgment in decision-making, human error, control processes being deliberately circumvented by employees and others, management overriding controls, and the occurrence of unforeseeable circumstances.

Future periods

Our assessment of controls is at January 2026 only. Historic evaluation of effectiveness is not relevant to future periods due to the risk that:

- The design of controls may become inadequate because of changes in operating environment, law, regulation, or other changes; or
- The degree of compliance with policies and procedures may deteriorate.

Responsibilities of management and internal auditors

It is management's responsibility to develop and maintain sound systems of risk management, internal control, and governance, and for the prevention and detection of irregularities and fraud. Internal audit work should not be seen as a substitute for management's responsibilities for the design and operation of these systems.

We endeavor to plan our work so that we had a reasonable expectation of detecting significant control weaknesses and, if detected, we carried out additional work directed towards identification of consequent fraud or other irregularities. However, internal audit procedures alone, even when carried out with due professional care, do not guarantee that fraud will be detected.

Accordingly, our examinations as internal auditors should not be relied upon solely to disclose fraud, defalcations, or other irregularities which may exist.

Thank you

PricewaterhouseCoopers LLP is a limited liability partnership registered in England with registered number OC303525. The registered office of PricewaterhouseCoopers LLP is 1 Embankment Place, London WC2N 6RH. PricewaterhouseCoopers LLP is authorised and regulated by the Financial Conduct Authority for designated investment business and the Solicitors Regulation Authority for the provision of regulated legal services.

This document has been prepared only for Tayside Pension Fund and solely for the purpose and on the terms agreed with Tayside Pension Fund in our agreement dated 20 January 2025. We accept no liability (including for negligence) to anyone else in connection with this document, and it may not be provided to anyone else.

© 2026 PricewaterhouseCoopers LLP. All rights reserved. 'PwC' refers to the UK member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.



Tayside Pension Fund (TPF)

McCloud Post-Implementation Review

Final Report

This page is intentionally left blank

Contents

1 Executive Summary (Pages 3-5)

2 Findings (Pages 6-8)

3 Appendices (Pages 9-15)

Appendix A: Basis of Classifications

Appendix B: Terms of reference extract: Audit scope and approach

Appendix C: Limitations and Responsibilities

This page is intentionally left blank

Executive Summary

Report classification

Satisfactory with exceptions

Refer to Appendix A for the basis of classification

	Critical	High	Medium	Low	Advisory
Audit identified	-	1	-	-	-

Background and Scope

This review was conducted in accordance with the extension of the FY26 internal audit plan approved by the Pensions Committee and was intended to provide independent assurance over the design effectiveness of controls supporting McCloud post-implementation within the Tayside Pension Fund (“TPF” / “the Fund”).

The McCloud remedy was introduced to address age discrimination identified in public sector pension schemes following the McCloud judgment. For Local Government Pension Scheme (LGPS) funds, this requires pension administration processes to identify eligible members, assess whether underpin protection applies, calculate any relevant McCloud underpin position, and ensure that member records, calculations and communications are updated appropriately.

Given the complexity of the remedy, the Fund’s control framework is expected to ensure that McCloud-related processing is supported by clear system guidance, accurate member and employer data, appropriate calculation methodology, effective Quality Assurance (QA), defined escalation routes, staff training, and member communications aligned to regulatory expectations. Effective controls are therefore important to reduce the risk of incorrect member outcomes, delayed processing, inconsistent treatment of cases, or inaccurate communications.

This audit assessed the design of controls supporting McCloud Business as Usual (BAU) processing across key areas, including eligibility identification, data validation, calculation methodology, calculation review and approval, manual processing, issue and exception management, training, governance, supplier interaction with Heywood / Altair, and member communications. The objective was to determine whether TPF has designed appropriate arrangements to support accurate, consistent and controlled McCloud processing within BAU pension administration.

Conclusion

Overall, TPF has established a proportionate control design framework over McCloud BAU processing, with key activities evidenced through walkthroughs and supporting examples across eligibility assessment, data review, calculation processing, review, communications, exception handling and escalation. This review identified one High-rated finding, relating to enhancements required to strengthen the McCloud BAU documentation and governance framework. The finding does not indicate the absence of key controls, as TPF evidenced control design through walkthroughs, workflow examples, guidance, training material, communication templates and case examples. Rather, it reflects the need to more fully align the BAU McCloud Process Notes and related manual processing guidance with the control activities evidenced during the review, to support consistency, auditability and sustainability as McCloud activity continues to move into BAU.

Executive Summary

Headlines

The internal audit of Tayside Pension Fund's McCloud BAU control framework identified that key McCloud processing activities have been designed and evidenced through walkthroughs and supporting examples. Core activities — including eligibility assessment, data review, calculation processing, review, communications, exception handling and escalation — were evidenced as part of the control design assessment; however, enhancements are required to strengthen formal BAU documentation, clarify governance arrangements and improve the consistency and auditability of the control design.

As part of our audit, we reviewed the McCloud BAU control framework and associated control environment. The finding identified indicates that while TPF has established key practical controls, the BAU McCloud Process Notes and related manual processing guidance do not yet fully reflect the end-to-end control design. Enhancements are therefore required to align documented procedures with the control activities evidenced during the review, including clearer documentation of processing steps, roles and responsibilities, calculation review controls, communication issue controls, error and escalation handling, training arrangements, governance oversight and future document review arrangements.

Summary of findings:

- **McCloud BAU Control Framework Documentation** (*High*): The McCloud BAU control framework includes key control activities evidenced through walkthroughs, Altair workflow examples, Heywood guidance, training material, communication templates, training records and case examples. However, these activities are not consistently captured within the BAU McCloud Process Notes and related manual processing guidance, resulting in a gap between the control activities evidenced during the review and the procedures formally documented for BAU operation. This includes documentation gaps across the end-to-end BAU processing flow, roles and responsibilities, calculation QA and review, manual intervention controls, communication selection and issue, errors / warnings / escalation handling, training governance, senior management oversight and future document review arrangements.

Executive Summary

Areas of Good Practice

We also identified the following areas of good practice during our review:

1. Completion of McCloud Data Readiness and Cleansing Activity Prior to BAU Processing

TPF undertook data readiness and cleansing activity to support the transition of McCloud processing into BAU. This included review of data interface uploads, data validity outputs and service history exceptions, with issues investigated and progressed as part of preparation for BAU processing. This helped establish a stronger data foundation for McCloud processing.

2. Practical Validation of McCloud Processing Prior to BAU Transition

TPF performed practical checks of McCloud processing outputs in the test and live environments as part of implementation assurance. Testing identified examples of TPF reviewing McCloud tranche, rectification and calculation outputs before the process was embedded into BAU. This supported the design and implementation of McCloud processing controls.

3. Active Employer Engagement to Resolve Member Data Queries

TPF demonstrated active engagement with employers where additional or clarified information was required for McCloud processing. Examples reviewed showed queries being raised in relation to service history, part-time additional hours and other member data points, with cases progressed once responses were received. This supports the completeness and accuracy of member data used in McCloud calculations.

4. Delivery of Detailed McCloud Training and Knowledge Sharing

TPF delivered McCloud training and knowledge-sharing activity to support staff involved in McCloud processing. This included structured training sessions, practical demonstrations and supporting materials covering key McCloud processing areas. This helped build staff understanding of McCloud requirements and supported the transition of processing responsibilities into BAU.

5. Evidence of Case-Level Review within the BAU Process

Walkthroughs and case examples demonstrated that case-level review activities are incorporated within the McCloud BAU process. Examples reviewed included independent checking of calculation outputs, review of service history information and challenge of incomplete employer data before cases were progressed. This supports the design of review controls within the BAU process.

This page is intentionally left blank

Current-year Findings

1

McCloud BAU Control Framework Documentation

Control Design

Finding rating

Impact	Highly significant
Likelihood	Probable
Rating	High

Findings

Overall, TPF has established a proportionate control design framework to support McCloud BAU processing. Key control activities were evidenced through walkthroughs and supporting examples across eligibility assessment, data review, calculation processing, review, communications, exception handling and escalation. The review identified one key theme, relating to opportunities to further strengthen the formal McCloud BAU documentation and governance framework. The finding does not indicate the absence of key controls. Rather, it reflects a gap between the control activities evidenced during the review and the procedures formally documented within the BAU McCloud Process Notes and related manual processing guidance. Addressing this will support improved consistency, auditability and sustainability as McCloud processing continues to be embedded into BAU.

Our review specifically noted the documentation gaps as follows:

- **End-to-end BAU processing flow is not fully captured**, as the BAU McCloud Process Notes document elements of the process but do not describe the complete flow from source data review through to calculation, review and communication / payment issue. This includes the expected checks over employer data, service history, pensionable pay, additional hours, service gaps, career breaks, McCloud tranche / rectification processing and transfer calculation review.
- **Roles and responsibilities across the BAU McCloud process are not fully captured**, although these are understood in practice. This includes roles of the BAU processing team and other teams involved in calculation preparation, checking, approval, escalation, communication issue, retrospective calculations, training oversight and maintenance of process documentation.
- **Calculation QA, review and manual intervention controls are not fully defined**, although calculation review and segregation of duties were identified through walkthrough and Altair task examples. The written procedures do not fully set out when calculations require Senior Pension Assistant review, how preparer / checker responsibilities are assigned, how segregation of duties is maintained, and what review / approval steps are required before calculation outputs, transfer values or payment instructions are released. The retrospective / manual processing notes also do not fully capture when manual or non-standard actions require review or approval, or how independence of review is maintained.
- **McCloud communication selection and issue controls are not fully embedded within the BAU Process Notes**, although TPF provided separate McCloud paragraph guidance for scenario-based wording. The BAU notes do not fully cross-reference this guidance or describe how staff should select the relevant template / paragraph, check member communication preference / Pension Portal status where relevant, apply review where required, and confirm issue through the appropriate route.

Current-year Findings

1

McCloud BAU Control Framework Documentation

Control Design

Findings (Continued)

- **McCloud errors, warnings, exceptions and escalation steps are not fully set out in the BAU notes**, although TPF explained the escalation route to a Senior Pension Assistant, the TPF IT Team and Heywood where a system-related issue is suspected. The BAU notes refer staff to a separate errors / warnings document, but do not clearly explain how that document should be used, which errors / warnings require escalation, when matters should be escalated to the TPF IT Team / Heywood, or what should be recorded in the Altair task when an error, warning or exception is identified.
- **Training arrangements are not yet comprehensively documented**, although training materials and a training log were available. The training record is not yet comprehensive, and the documentation does not fully define refresher training expectations, new starter training arrangements or how training completion is monitored as McCloud becomes embedded into BAU.
- **Governance and oversight arrangements have not been fully formalised**, although McCloud matters are discussed through management and team routes. The documentation does not define the formal senior management governance route for McCloud as a BAU subject matter, including oversight of the BAU processing lifecycle, operational progress, key risks, regulatory / guidance updates, action ownership and management review.
- **Document ownership, approval and future review arrangements are not clearly defined**, as the BAU Process Notes do not identify document ownership, formal approval for BAU use, review frequency, or a documented process for assessing and incorporating future regulatory, statutory, tax or guidance updates into BAU procedures. Given the complexity of McCloud calculations, case types and regulatory dependencies, defined ownership and update arrangements are expected to ensure the guidance remains current and consistently applied. As this is the first version of the document, the absence of version history or a change log has not been treated as a gap.

Overall, TPF has designed key practical controls to support McCloud BAU processing. The finding therefore relates to strengthening the formal documentation framework so that the control design is clearly evidenced, repeatable and sustainable as McCloud activity continues to move into BAU.

Implications

While TPF has evidenced key McCloud BAU controls through walkthroughs and supporting examples, incomplete and not yet formally approved BAU documentation may reduce consistency, auditability and sustainability over time. Reliance on staff knowledge, walkthrough explanations and individual workflow notes may increase the risk that McCloud processing, calculation review, manual interventions, communications, exception handling, escalation and governance activities are applied inconsistently, particularly as responsibilities move further into BAU or where new staff become involved.

A more complete and formally governed BAU documentation framework would help ensure that roles, review points, control steps, escalation routes and update responsibilities are clearly understood, consistently applied and capable of audit.

Current-year Findings

1

McCloud BAU Control Framework Documentation

Control Design

Recommendations

TPF should update the BAU McCloud Process Notes and related manual processing guidance to reflect the control activities evidenced during the review and support consistent application across the McCloud BAU process. This should include:

1. **Documenting the end-to-end BAU process**, from source data review through to calculation, review, communication and payment issue, including key checks over employer data, service history, pensionable pay, additional hours, service gaps, career breaks, McCloud tranche / rectification processing and transfer calculations.
2. **Defining roles and responsibilities** for the BAU processing team and other teams involved in McCloud activities, including calculation preparation, checking, approval, escalation, communications, retrospective calculations, training oversight and maintenance of process documentation.
3. **Formalising calculation QA and manual intervention controls**, including Senior Pension Assistant review triggers, preparer / checker responsibilities, segregation of duties, approval steps before release of calculation outputs, transfer values or payment instructions, and review of manual or non-standard actions.
4. **Embedding communication control steps within the BAU Process Notes**, including cross-reference to the McCloud paragraph guidance, template selection, member communication preference / Pension Portal checks where relevant, review requirements and confirmation of issue through the appropriate route.
5. **Clarifying error, warning, exception and escalation procedures**, including use of the separate errors / warnings guidance, escalation triggers to a Senior Pension Assistant, the TPF IT Team or Heywood, and expected Altair task notes where issues are identified.
6. **Enhancing training governance**, including completion records, refresher training triggers, new starter requirements and monitoring of McCloud training completion as part of BAU.
7. **Formalising senior management oversight of McCloud**, including review of BAU processing progress, key risks, regulatory / guidance updates, action ownership and management reporting.
8. **Establishing document ownership, approval and review arrangements**, including document owner, formal approval for BAU use, review frequency, and a documented process for assessing and incorporating future regulatory, statutory, tax or guidance updates into BAU procedures. As this is the first version, version control and change-log arrangements should apply to future updates.

Management Actions

Management acknowledges this gap, and resource is currently being reviewed in the staffing structure to assist.

Responsible person/title:
Amanda Smith,
Corporate Finance, Pensions Team Leader

Due Date
31st March 2027

This page is intentionally left blank

Appendices

Appendix A: Basis of our classifications

Appendix B: Terms of reference extract - Audit scope and approach

Appendix C: Limitations and Responsibilities

This page is intentionally left blank

A) Basis of Classifications

Individual finding ratings

Likelihood \ Impact	Critical	Highly Significant	Major	Moderate	Minor	Insignificant
Highly likely	Critical	Critical	High	High	Medium	Medium
Likely	Critical	High	High	Medium	Medium	Low
Probable	High	High	Medium	Medium	Low	Low
Possible	High	Medium	Medium	Low	Low	Low
Unlikely	Medium	Medium	Low	Low	Low	Not reportable
Not expected	Medium	Low	Low	Low	Not reportable	Not reportable

Report classifications

The report classification is determined by allocating points to each of the findings included in the report.

Findings rating	Points
Critical	40 points per finding
High	10 points per finding
Medium	3 points per finding
Low	1 point per finding

Report classification	Points
 Satisfactory	6 points or less
 Satisfactory with exceptions	7 – 15 points
 Needs improvement	16 – 30 points
 Unsatisfactory	31 points and over

This page is intentionally left blank

B) Terms of reference extract: Audit scope and approach (1/4)

Background

This review is being conducted in accordance with the extension of the FY26 internal audit plan approved by the Pensions Committee and will provide assurance over the effectiveness of controls supporting the post-implementation of the McCloud remedy within Tayside Pension Fund (“TPF” / “the Fund”).

TPF is a Local Government Pension Scheme (LGPS) administering authority in Scotland, providing defined benefit (DB) pensions to eligible employees of participating employers in the Tayside region. The Fund is overseen by the Pension Fund Committee, supported by a Pension Board, with responsibility for governance, administration, and regulatory compliance. Day-to-day delivery is supported by internal teams and key third-party providers, including administrators, actuaries, and system vendors.

The McCloud remedy addresses age discrimination arising from transitional protections in public sector pension reforms. It requires schemes to identify affected members, recalculate benefits for the remedy period (2015–2022), and issue revised communications. Implementation is a complex, data-driven programme with dependencies across member data, system configuration, calculation processes, and third-party delivery.

Robust governance, data controls, system implementation, and third-party oversight are therefore critical to ensure the remedy is delivered accurately, in line with regulatory requirements and timelines, and without adverse impact to members.

Audit objective

The objective of this audit is to assess controls across the end-to-end McCloud post-implementation process at Tayside Pension Fund, including member identification, data management, calculation governance, system processing, third-party delivery, and member communications.

An estimated **15 audit days** have been allocated for this review. The work will be primarily desk-based, supported by targeted discussions and walkthroughs with key stakeholders, with relevant documentation and evidence provided by the Fund.

B) Terms of reference extract: Audit scope and approach (2/4)

We will review the design effectiveness of key controls in place over McCloud post-implementation. The processes, risks and related control objectives included in this review are:

Audit Scope Area	Control Objectives	Key Risks
Member Identification & Data Integrity	- McCloud-eligible members are identified using approved logic, with the final population subject to validation and sign-off prior to operational reliance. - Key McCloud data (including employer payroll inputs, service history, and membership status) is subject to reconciliation to pension records, with processes in place to investigate and resolve variances. - Data issues are tracked through a defined process, with mechanisms in place to monitor and resolve items, including identification of any material outstanding issues.	- Member identification logic is not adequately defined or consistently applied, resulting in risk of incorrect population. - Controls over key data are not adequately designed, resulting in risk of inaccurate inputs. - Data issues are not effectively tracked or resolved, resulting in risk to member outcomes
Calculation Governance & Quality Assurance (QA) and Output Validation	- McCloud calculation methodology is defined and applied in line with approved logic and system configuration. - QA controls are in place over calculation outputs, including review, exception handling, and resolution prior to operational use - Manual adjustments or exceptions are subject to logging, review, and approval controls.	- Calculation methodology is not adequately defined or consistently applied, resulting in risk of errors in outputs. - QA controls are not adequately designed or effectively operating, resulting in risk of errors not being identified. - Controls over manual adjustments are not effective, resulting in risk of inappropriate changes.

B) Terms of reference extract: Audit scope and approach (3/4)

Audit Scope Area	Control Objectives	Key Risks
Systems Processing & Data Integration	• System configurations supporting McCloud processing are aligned to approved requirements. • System processing of McCloud cases is supported by controls to identify, track, and resolve defects or processing errors. • Data transfers between employer payroll and pension systems are subject to controls to ensure completeness and accuracy.	• System configurations are not aligned to approved requirements, resulting in risk of processing errors. • Processing controls are not adequately designed to identify defects, resulting in risk of unresolved issues. • Interface controls are not adequately designed, resulting in risk of incomplete or inaccurate data transfers.
Third-Party Delivery & Operational Capability	• Roles and responsibilities between the Fund and third parties (administrator, actuary, system providers) are clearly defined. • Staff involved in McCloud processing are supported by training and guidance to perform their roles. • Third-party delivery is subject to performance monitoring, with processes to identify, escalate, and resolve issues.	• Roles and responsibilities are not clearly defined, resulting in risk of control gaps. • Training and guidance are not adequate, resulting in risk of inconsistent execution. • Third-party performance is not effectively monitored, resulting in risk of delays or errors.
Member Communications & Regulatory Compliance	• McCloud member communications (including Remediable Service Statements and benefit updates) are generated using approved outputs and are subject to review and approval prior to issuance. • Processes are in place to ensure communications are issued to the correct member population in line with regulatory requirements and timelines. • Compliance with McCloud regulatory requirements, including statutory guidance and associated tax considerations, is subject to monitoring processes.	• Controls over member communications are not adequately designed, resulting in risk of inaccurate outputs. • Processes for issuing communications are not effective, resulting in risk of incorrect or delayed issuance. • Compliance monitoring is not effective, resulting in risk of regulatory non-compliance.

B) Terms of reference extract: Audit scope and approach (4/4)

Limitations of Scope

This audit is limited to the scope outlined above and will rely on information and evidence provided by Fund management and relevant third parties and will not independently re-perform or validate all underlying source data. The following areas are out of scope:

- Re-performance of McCloud benefit calculations, including validation of underpin calculations or individual member outcomes.
- Actuarial methodology assurance, including validation of assumptions, models, or technical judgements.
- Detailed validation of underlying data at member level, including eligibility, full verification of historical pay, service, or membership records.
- Execution of data remediation activities, including cleansing or reconstruction of incomplete or inconsistent data.
- Detailed tax validation, including independent review of annual allowance or other tax calculations arising from McCloud processing.
- Broader IT general controls or full system lifecycle reviews, beyond McCloud-specific configurations and processing.
- Independent assurance over third-party internal control environments, beyond assessing the Fund's oversight arrangements.
- Legal interpretation of regulations or scheme rules, including formal assessment of advice obtained by the Fund.
- Verification of the accuracy of individual member communications or statements issued, including Remediable Service Statements or benefit outputs.
- Forward-looking assurance over the ongoing success of the McCloud programme, including guarantees over timelines or absence of future errors.

Audit approach

At the outset of the review, we will engage with key stakeholders to obtain an understanding of TPF's McCloud post-implementation framework, including governance arrangements, key third-party dependencies, and how risks are managed in practice. Our approach will include the following activities:

- Conduct walkthroughs with relevant personnel to understand McCloud processes, controls, and responsibilities across TPF and key third parties.
- Review relevant documentation and management information to assess the design of controls supporting member identification, data management, calculation processes, system configuration, and governance.
- Evaluate the design effectiveness of key controls to determine whether they are appropriately structured to mitigate identified risks.
- Discuss findings with management to validate observations, understand root causes, and agree practical actions.
- Prepare a draft and final report summarising findings, good practices, and recommendations.

C) Limitations and responsibilities

Limitations inherent to the internal auditor's work

This internal audit has been conducted subject to the inherent limitations associated with internal audit work and internal control systems more generally.

Internal control systems, no matter how well designed, are subject to inherent limitations. These include, but are not limited to, the risk of human error, poor judgement in decision-making, deliberate circumvention of controls by employees or third parties, management override of controls, and the occurrence of unforeseeable circumstances. Accordingly, internal audit procedures cannot provide absolute assurance that all control weaknesses, errors, fraud, or other irregularities will be detected.

Our work has been planned and performed to obtain reasonable, but not absolute, assurance that the key controls within scope are designed effectively to mitigate the relevant risks.

Future periods

Our assessment of controls is for the post-implementation phase of McCloud effective 1st Nov'25 i.e., the BAU phase. The evaluation of the design effectiveness of controls during this period should not be relied upon as evidence that the control design will remain appropriate in future periods.

This is because:

- The design of controls may become inadequate due to changes in the operating environment, regulation, legal requirements, or business activities; and
- The extent to which procedures remain aligned to the control design may change over time.

Responsibilities of management and internal auditors

Management is responsible for establishing and maintaining effective systems of risk management, internal control, and governance, including controls designed to prevent and detect errors, irregularities, and fraud. Internal audit does not relieve management of these responsibilities, nor should it be considered a substitute for management's own control activities.

Internal audit plans and performs its work with the objective of having a reasonable expectation of identifying significant control weaknesses and, where identified, undertaking additional procedures directed towards understanding the potential impact. However, internal audit procedures alone, even when carried out with due professional care, do not guarantee that fraud or other irregularities will be detected.

Accordingly, reliance should not be placed solely on the work of internal audit to identify all instances of fraud, defalcation, or other irregularities that may exist.

Thank you

PricewaterhouseCoopers LLP is a limited liability partnership registered in England with registered number OC303525. The registered office of PricewaterhouseCoopers LLP is 1 Embankment Place, London WC2N 6RH. PricewaterhouseCoopers LLP is authorized and regulated by the Financial Conduct Authority for designated investment business and the Solicitors Regulation Authority for the provision of regulated legal services.

This document has been prepared only for Tayside Pension Fund and solely for the purpose and on the terms agreed with Tayside Pension Fund in our agreement dated 1st April 2026. We accept no liability (including for negligence) to anyone else in connection with this document, and it may not be provided to anyone else.

© 2026 PricewaterhouseCoopers LLP. All rights reserved. 'PwC' refers to the UK member firm and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.



Data Quality Review

Tayside Pension Fund

A large, solid orange decorative bar is positioned horizontally across the lower half of the slide. It is composed of two parallel slanted rectangular segments joined together, creating a continuous zig-zag shape.

June 2026

This page is intentionally left blank

Contents

- 1 Purpose, scope and approach *(Pages 3-5)*
- 2 Findings from data quality review *(Pages 6-10)*

Appendices

Appendix 1: Critical Risk Observations *(Pages 12-16)*

Appendix 2: Medium Risk Observations *(Pages 17-21)*

Appendix 3: Low Risk Observations *(Pages 22-26)*

Appendix 4: Important Notes *(Pages 27-32)*

Appendix 5: Terms of Reference (ToR) *(Pages 33-36)*

Distribution list

For action:

Stuart Norrie (Senior Banking & Investment Officer)

Amanda Smith (Pension Team Leader, Operations)

This page is intentionally left blank

1

Purpose, scope and approach

This page is intentionally left blank

Background and purpose

Background

Ensuring high-quality data is fundamental to the effective management, governance, and administration of the pension scheme. Accurate, complete, and consistent data form the foundation upon which all key pension processes depend, - from calculating and paying member benefits to meeting statutory and regulatory reporting obligations. Reliable data enables administrators and trustees to deliver timely and correct benefits, maintain compliance with legislation, and make well-informed strategic decisions regarding funding, investment, and risk management.

Purpose

This report is addressed to and for the attention of the Dundee City Council in their role of administering the Scheme. It sets out the results of internal audit's Data Gap Analyser ('DGA') for the member data provided for the Scheme.

The purpose of our work is to assess whether the data is sufficiently complete and internally consistent to support future Scheme activity. Our work focuses on data quality and explainability; it is not a legal verification of benefit entitlements. We have relied on the data provided to us and have not verified it against original source documents.

As PwC does not hold the Scheme's benefit specification, we have not performed checks to compare the data with the benefit specification and have not undertaken recalculations of member benefits to verify that benefits have been calculated correctly under the Scheme rules.

This report summarises:

- the data received and populations covered (deferred, pensioners and dependant members);
- the tests performed and results at a headline level;
- the key data issues identified (prioritised by risk), including where an interpretation is not evidenced by the data and is therefore recorded as a limitation / assumption; and
- recommended next steps to address the most material gaps.

Data received and populations

PwC received the membership data extract(s) on 30 April 2026. Our review was performed on the membership data extract(s) provided for the purpose of this exercise, covering 11944 records for deferred members, 17415 records for pensioner members and 3011 records for dependant members.

Approach to review and navigating our findings

How to read the findings

The tables within this report summarise the data gaps identified for deferred, pensioner and dependant records. The purpose is not only identifying gaps, but also understanding their potential impact on benefit payments to the members and the recommended next steps.

Risk categorisation

We have categorised the gaps identified as follows:

- **Critical Observations** - Gaps that could materially impact on the benefits the member is receiving and / or the valuation of their benefits.
- **Medium Risk Observations** - Gaps that could materially impact on the valuation of benefits today and which we expect will be resolved on future member events and / or where reasonable assumptions could be made.
- **Low Risk Observations** - Gaps that are expected to have low or no impact on benefits and are likely due to data not being fully recorded.

Each issue identified in the following section includes an estimate of the number of records affected and suggested next steps to resolve these issues. Where the data does not have a clear interpretation (for example, where the time period of a tranche cannot be determined from the extract alone), we record this explicitly as a limitation / assumption.

2

Findings from data quality review

This page is intentionally left blank

Output of the review

Conclusions from data quality review

Based on the data extracts provided, the Scheme data is generally in good shape given the limited number of tests with failures that are classified as critical gaps. The critical gaps are mostly related to inconsistencies between pension tranches and members' service dates for deferred and pensioner members, inconsistencies in retirement type for pensioners and a number of duplicate entries in the dependant member data. We have also identified a number of non-critical areas where data quality can be improved. Recommended data cleansing actions include:

- File reviews for small populations, including where the pension tranching and service dates are inconsistent.
- Tracing to determine whether members are still alive, particularly the older deferred members who have yet to retire and the older pensioner and dependant members.
- A write out to and targeted tracing of pensioner members to request spouse information where it is missing.
- Sample review of the largest populations to validate the tranching of pension benefits, inconsistencies in retirement types and the duplicate dependant members.

Next steps

- Management to review the data observations and key assumptions / limitations set out in this report, and consider whether there are any obvious explanations for the failed tests.
- Management should consider whether any data improvement work or sample checking is required.
- Management should report back to the Pensions Committee on work performed and the results this – addressing the findings of this report.

This page is intentionally left blank

Deferred population – data gap summary

Set out below is a summary of the analysis carried out for the deferred member population, with issues categorised by risk rating. 'No. of records impacted' reflects the number of field-level test failures identified (members may contribute multiple failures).

The numbers in the report reflect the number of records with issues. There may be multiple issues on the same record and are therefore counted more than once in the aggregated numbers.

Risk rating	No. of tests with failures	No. of records impacted (aggregate)	Comments	Next steps
Critical Risk Material impact	5	90	The critical issues identified relate to inconsistencies between the pension tranches and members' service dates. In addition, 20 deferred members were over age 75 at the date of the data extract.	We recommend a file review for the inconsistent pension tranches and a tracing exercise is carried out to identify whether the pension for the older deferred members should be in payment.
Medium Risk Less material impact	14	522	The medium risk data gaps relate to missing personal details and inconsistent membership data e.g. Date of Joining or Leaving the Company and Scheme and transfers-in data. We have also identified one duplicate record.	We recommend a tracing exercise or file reviews are carried out to resolve these issues.
Low Risk No / low impact	1	49	The low-risk data gap relates to a number of members with trivial pensions (<£10 p.a.).	The admin team may wish to review the files for these members. We expect these to be resolved as members retire.

Pensioner population – data gap summary

Set out below is a summary of the analysis carried out for the pensioner member population, with issues categorised by risk rating. 'No. of records impacted' reflects the number of field-level test failures identified (members may contribute multiple failures).

The numbers in the report reflect the number of records with issues. There may be multiple issues on the same record and are therefore counted more than once in the aggregated numbers.

Risk rating	No. of tests with failures	No. of records impacted (aggregate)	Comments	Next steps
Critical Risk Material impact	12	4827	Most of the critical issues relate to inconsistencies between the pension tranches and members' service dates, in particular the GMP pension tranches. We also identified some missing / invalid postcodes and transfers-in data.	We recommend file reviews for the largest populations impacted and a tracing exercise for members with missing / invalid postcodes.
Medium Risk Less material impact	6	4524	The medium risk issues mainly relate to dates of retirement being inconsistent with Date of Leaving, the implied retirement age being outside the expected range of 50-75 and inconsistencies in retirement types. We have also identified a small number of members above age 100 or who have trivial pensions (<£10 p.a.)	We recommend that a sample file review is undertaken to confirm the members' benefit entitlement and a tracing exercise to confirm the older pensioners are still alive.
Low Risk No / low impact	15	13091	These include missing details of members' marital status, spouse details (and pensions), rounding errors in GMP tranches and inconsistencies in membership dates.	These are likely to be non-critical data points from an operational and financial perspective. We recommend the headline findings are reviewed and rectification plans only implemented where deemed necessary.

**See Appendix 4 for further details on how we have interpreted the retirement types for pensioners.*

Dependant population – data gap summary

Set out below is a summary of the analysis carried out for the dependant member population, with issues categorised by risk rating. 'No. of records impacted' reflects the number of field-level test failures identified (members may contribute multiple failures).

The numbers in the report reflect the number of records with issues. There may be multiple issues on the same record and are therefore counted more than once in the aggregated numbers.

Risk rating	No. of tests with failures	No. of records impacted (aggregate)	Comments	Next steps
Critical Risk Material impact	5	601	Most of the critical issues relate to duplicated Member IDs. The remaining issues relate to missing / invalid postcodes and inconsistencies in the sum of the pension tranches.	We recommend a sample file review of the duplicate Member ID records and member tracing to confirm members with missing / invalid postcodes are still alive.
Medium Risk Less material impact	3	40	Most of the medium risk issues relate to the age of dependant members being outside the range we expect e.g. 18 to 100 for spouse dependants and <23 for child dependants.	We recommend member tracing to confirm that the older members are still alive and that the child dependants remain eligible to receive a dependant pension.
Low Risk No / low impact	3	158	These include missing details relating to the original member.	These are likely to be non-critical data points from an operational and financial perspective. No recommended actions.

This page is intentionally left blank

A large, bold, orange letter 'A' is positioned on the left side of the slide. It is a simple, sans-serif font with a thick stroke.

Appendices - Further details on failed tests

This page is intentionally left blank

1

Appendix 1 – Critical Risk Observations

This page is intentionally left blank

Critical Risk Observations

Deferreds

Test No.	Observation point	No. records impacted	Description	Additional Comments
Def 1	Total Revalued pre 2015 Deferred Pension (£ p.a.) (Blank)	4	Details held on file for Total Revalued pre 2015 Deferred Pension is blank where such benefit is expected based on service dates.	- Given the relatively small number of members impacted, we would typically resolve this population via file reviews.
Def 2	Total Revalued pre 2015 Deferred Pension (£ p.a.)	43	Details held on file for Total Revalued pre 2015 Deferred Pension is included where such benefit is not expected based on service dates.	
Def 3	Total Revalued post 2015 Deferred Pension (£ p.a.) (Blank)	9	Details held on file for Total Revalued post 2015 Deferred Pension is blank where such benefit is expected based on service dates.	
Def 4	Total Revalued Pension	14	The Total Revalued Deferred Pension does not match the sum of the Total Revalued pre and post 2015 Deferred Pensions in the data.	
Def 5	Date of Birth (reasonable)	20	Records where the member's age in the dataset is older than 75 while still being a deferred member.	- We recommend that the member are traced, with existence tracing used to confirm that they are still alive, if not already in progress.

Critical Risk Observations

Pensioners

Test No.	Observation point	No. records impacted	Description	Additional Comments
Pen 1	Postcodes	168	Records where postcode is not populated. We note that this may be as a result of the member being overseas and so not having a UK postcode recorded.	- We recommend that the members are traced, with existence tracing used to confirm that they are still alive.
Pen 2	Postcodes	124	Records where postcode is not contained within the most recent version of the ONS Postcode Directory.	
Pen 3	Pre 2015 Pension	234	Details held on file for pre 2015 Pension Amount (£ p.a.) at valuation date is included where such benefit is not expected based on service dates.	- For pension tranches where a small number of members are impacted, we would typically resolve this population via file reviews. - Where a larger number of members are impacted, you may wish to instead consider reviewing a sample of files for this population.
Pen 4	Pre 2015 Pension (Blank)	13	Details held on file for Pre 2015 Pension Amount (£ p.a.) at valuation date is blank where such benefit is expected based on service dates.	
Pen 5	Post 2015 Pension (Blank)	10	Details held on file for Post 2015 Pension Amount (£ p.a.) at valuation date is blank where such benefit is expected based on service dates.	
Pen 6	Pre 88 GMP	1233	Details held on file for Pre 88 GMP Pension Amount (£ p.a.) is included where such benefit is not expected based on service dates. We note that 922 of these members have a transfer in, while 311 do not.	
Pen 7	Pre 88 GMP (Blank)	659	Details held on file for Pre 88 GMP Pension Amount (£ p.a.) is blank where such benefit is expected based on service dates.	

**See Appendix 4 for further details on how we have interpreted the stated retirement types and the assumed normal retirement ages for members*

Critical Risk Observations

Pensioners

Test No.	Observation point	No. records impacted	Description	Additional Comments
Pen 8	Post 88 GMP	1012	Details held on file for Post 88 GMP Pension Amount (£ p.a.) is included where such benefit is not expected based on service dates. We note that 980 of these members have a transfer in, while 32 do not.	- For pension tranches where a small number of members are impacted, we would typically resolve this population via file reviews. - Where a larger number of members are impacted, you may wish to instead consider reviewing a sample of files for this population.
Pen 9	Post 88 GMP (Blank)	1120	Details held on file for Post 88 GMP Pension Amount (£ p.a.) at valuation date is blank where such benefit is expected based on service dates.	
Pen 10	Total Pension at valuation date	65	Total Pension at valuation date does not match the sum of the Pre and Post 2015 Pension Amounts.	
Pen 11	Transfer-in values	188	• There are 11 records with a date for a transfer-in but no transfer value amount. • The remaining 177 records have a date for a transfer-in but with a trivial transfer value (<£2 p.a.).	- Given the relatively small number of members impacted, we would typically resolve this population via file reviews.
Pen 12	Current AVC Pension	1	Record where the Current AVC Pension is lower than the Initial AVC Pension	- We recommend that a file review is undertaken to confirm the members' benefit entitlement.

Critical Risk Observations

Dependants

Test No.	Observation point	No. records impacted	Description	Additional Comments
Dep 1	Member ID	549	Records with duplicated Member IDs. Within these records there are 259 unique Member IDs and 290 duplicates. We have noted that this is the case where the original members have multiple periods of service. For example, dependant member 1067391 has two sets of duplicate records (4 in total), which are linked to two Original Member IDs 7166316855, 7166316857 respectively, who appear to be the same individual based on their personal details.	- We recommend a sample file review of the duplicate Member ID records with similar pension amounts and member details, to understand the reason for these duplicate records.
Dep 2	Postcodes	35	Records where postcode is not populated. We note that this may be as a result of the member being overseas and so not having a UK postcode recorded.	- We recommend that the members are traced, with existence tracing used to confirm that they are still alive.
Dep 3	Postcodes	15	Records where postcode is not contained within the most recent version of the ONS Postcode Directory.	
Dep 4	Total Pension at valuation date	1	Records where the Total Pension at the valuation date is not populated.	- Given the relatively small number of members impacted, we would typically resolve this population via file reviews.
Dep 5	Total Pension at valuation date (consistency)	1	Records where the Total Pension at the valuation date does not match the sum of the pre and post 2015 pension.	

2

Appendix 2 - Medium Risk Observations

This page is intentionally left blank

Medium Risk Observations

Deferreds

Test No.	Observation point	No. records impacted	Description	Additional Comments
Def 6	Date of Joining Company	3	Records where the Date of Joining Company has not been populated.	- Where a small number of members are impacted, we would typically resolve this population via file reviews. - Where a larger number of members are impacted, you may wish to instead consider reviewing a sample of files for this population.
Def 7	Date of Joining Company (reasonable)	10	Records where the Date of Joining Company and the member's age at this date is not sensible i.e. the member is not between age 16 and 65.	
Def 8	Date of Joining Company (consistency)	2	Records where the Date of Joining Company is not consistent with other date entries i.e. the Date of Joining Company is not between the Date of Birth and the Date of Leaving Scheme.	
Def 9	Date of Joining Scheme (reasonable)	9	Records where the Date of Joining Scheme and the member's age at this date is not sensible i.e. the member is not between age 16 and 65.	
Def 10	Date of Joining Scheme (consistency)	1	Records where the Date of Joining Scheme is not consistent with other date entries i.e. the Date of Joining Scheme is not between the Date of Birth and the Date of Leaving Scheme.	
Def 11	Date of Leaving Scheme	39	Records where the Date of Leaving Scheme is not populated. We note that the majority of these relate to members with Pension Credits, except for 2 members.	
Def 12	Date of Leaving Scheme (consistency)	5	Records where the Date of Leaving Scheme is not consistent with other date entries i.e. the Date of Leaving Scheme is not after the Date of Birth, the Date of Joining Company and the Date of Joining Scheme.	
Def 13	Member contributions	74	Records where the member contributions are not populated.	

Medium Risk Observations

Deferreds

Test No.	Observation point	No. records impacted	Description	Additional Comments
Def 14	Transfer-in value	15	4 members have a date input for a transfer-in but no transfer-in amount. 9 members have a date input and a trivial transfer-in amount (<£2).	- Due to the small number of members impacted we would typically resolve this population via file reviews.
Def 15	Transfer-in date (consistency)	1	There is 1 member whose transfer in date is prior to the date they joined the Scheme	
Def 16	Duplicates	2	There are 2 records which have identical Date of Birth, Date of Joining Scheme, Date of Leaving Scheme, and initial pension amounts.	
Def 17	Postcodes	147	Records where there is no postcode populated. We note that this may be as a result of the member being overseas and so not having a UK postcode recorded.	- We expect that these will be resolved when the member retires
Def 18	Postcodes	135	Records where the postcode is not contained within the most recent version of the ONS Postcode Directory.	
Def 19	Marital Status*	79	Records where there is no marital status populated.	

*See Appendix 4 for further details on how we have interpreted the stated marital statuses for members

Medium Risk Observations

Pensioners

Test No.	Observation point	No. records impacted	Description	Additional Comments
Pen 13	Date of Birth (reasonable)	5	There are 5 members above age 100 at the Date of Data extract.	- We recommend that the members are traced, with existence tracing used to confirm that they are still alive.
Pen 14	Date of Retirement (reasonable)	584	Records where the Date of Retirement is not sensible i.e. the member's age is not between 50 and 75, excluding members who retired early due to ill health. We note that the majority of these members have no disclosed retirement types.	- We recommend that a file review is undertaken to confirm the members' benefit entitlement.
Pen 15	Date of Retirement (consistency)	29	Records where the Date of Retirement is not consistent with other date entries i.e. Date of Retirement is not after the Date of Birth, Date of Joining Company, Date of Joining Scheme and Date of Leaving Company.	
Pen 16	Trivial Total Pension	24	Records where the Total Pension is trivial (<£10 p.a.) and we would have expected it to be fully commuted at retirement rather than put into payment	
Pen 17	Retirement type	2583	Members where there is no retirement type input e.g. normal, late, early etc.	- Due to the large number of members impacted, you may wish to consider reviewing a sample of files for this population, to confirm the members' benefit entitlement.
Pen 18	Retirement type (consistency)	1299	Members whose retirement types are not consistent with their dates of retirement in the data provided.*	

*See Appendix 4 for further details on how we have interpreted the retirement types for members

Medium Risk Observations

Dependants

Test No.	Observation point	No. records impacted	Description	Additional Comments
Dep 6	Date of Birth (reasonable)	35	Records where the Date of Birth and the resulting age at the Date of Data is not sensible i.e. the member is between 18 and 100 if not a child dependant member, and below the child age threshold of 23 if a child dependant member.	- We recommend member tracing to confirm that the older members are still alive and that the child dependants remain eligible to receive a dependant pension.
Dep 7	Date of Death (consistency)	1	There is 1 dependant member where the original member's Date of Death is before the Date of Leaving Scheme.	- Due to the small number of members impacted we would typically resolve this population via file reviews.
Dep 8	Trivial Total Pension	4	Records where the Total Pension is trivial (<£5 p.a.) and we would have expected it to be fully commuted at retirement of original member rather than put into payment.	- We recommend that a file review is undertaken to confirm the members' benefit entitlement.

3

Appendix 3 - Low Risk Observations

This page is intentionally left blank

Low Risk Observations

Deferreds

Test No.	Observation point	No. records impacted	Description	Additional Comments
Def 20	Trivial total pension	49	Records where the Total Pension is trivial (<£10 p.a.) and we would have expected it to be fully commuted at retirement rather than put into payment.	- We recommend that a file review is undertaken to confirm the members' benefit entitlement.

Low Risk Observations

Pensioners

Test No.	Observation point	No. records impacted	Description	Additional Comments
Pen 19	Pre 88 GMP at current date rounding	1	Pre 88 GMP records which are not rounded to the statutory 52p.	- Due to the small number of members impacted we would typically resolve this population via file reviews.
Pen 20	Post 88 GMP at current date rounding	1	Post 88 GMP records which are not rounded to the statutory 52p.	
Pen 21	Marital Status*	43	Records where the marital status is not populated.	- We recommend a member write out exercise to improve the quality of data held.
Pen 22	Spouse - Date of Birth	4765	2252 records where the Spouse Date of Birth is not populated, excluding single and widowed members and members with no marital status. 2513 records where the Spouse Date of Birth is populated despite the member not being married	
Pen 23	Spouse - Date of Birth (consistency)	2743	Records where the implied age at the Date of Data is greater than 100, less than 18 or more than 10 years younger than the member. This includes one Spouse Date of Birth which is in the future.	
Pen 24	Total contingent spouse pension at current date	2502	- There is 1 record which has a negative CSP figure. - There are 2501 records where CSP is nil.	
Pen 25	Contingent spouse Pre 2015 pension amounts	2701	Records where the Pre 2015 CSP is not populated.	

*See Appendix 4 for further details on how we have interpreted the stated marital statuses for members

Low Risk Observations

Pensioners

Test No.	Observation point	No. records impacted	Description	Additional Comments
Pen 26	Initial AVC Pension	1	Record where the member has a Current AVC Pension but no Initial AVC Pension.	- We recommend that a file review is undertaken to confirm the members' benefit entitlement.
Pen 27	Date of Joining Company	2	Records where the Date of Joining Company is not populated.	
Pen 28	Date of Joining Company (reasonable)	134	Records where the member's age at the Date of Joining Company is either below 16 or above 65.	
Pen 29	Date of Joining Company (consistency)	41	Records where the Date of Joining Company is not consistent with other date entries e.g. Date of Joining Company is later than Date of Leaving Scheme.	
Pen 30	Date of Joining Scheme (reasonable)	116	Records where the member's age at the Date of Joining Scheme is either below 16 or above 65.	
Pen 31	Date of Joining Scheme (consistency)	33	Records where the Date of Joining Scheme is not consistent with other date entries e.g. Date of Joining Scheme is later than Date of Leaving Scheme.	
Pen 32	Date of Leaving Scheme	5	Records where the Date of Leaving Scheme is not populated.	
Pen 33	Total Tax Free Cash Sum is valid	3	Records where the amount of the Total Tax Free Cash Sum less than £0	

Low Risk Observations

Dependants

Test No.	Observation point	No. records impacted	Description	Additional Comments
Dep 9	Original member details missing	76	Records where the original member ID, gender and Date of Birth are not populated	- Not expected to be required.
Dep 10	Original member Date of Leaving Scheme	81	Records where the original member Date of Leaving Scheme is not populated	
Dep 11	Post 88 GMP at current date rounding	1	Post 88 GMP records which are not rounded to the statutory 52p.	- Due to the small number of members impacted we would typically resolve this population via file reviews.

4

Appendix 4 – Important Notes

This page is intentionally left blank

Assumptions made

Where we have had to assume how a data item should be interpreted, we set this out below. If any of these are not correct then please let us know and we can update our results as needed.

Key Assumptions.

- The normal retirement date for the member is their state pension date set out in the data provided (we have not sought to verify these) subject to a minimum normal retirement age of 65.
- We have assumed that pension tranches with references to pre 2014 / 2015 relate to pensionable service before 1 April 2015 and pension tranches with references to post 2014 / 2015 relates to pensionable service after 1 April 2015.
- Child age threshold is assumed to be 23.

Retirement types in data	PwC interpretation
N	Normal retirement
E	Early retirement
R	Early retirement
I	Ill health retirement
P	Early retirement
H	Early retirement
L	Late retirement
V	Early retirement
O	Early retirement
W	Early retirement

Marital statuses in data	PwC interpretation
M	Married
S	Single
P	Partner
D	Divorced
C	Common Law
W	Widow/Widower

Dependant benefit types	PwC interpretation
W	Widow/Widower
N	Nominated
C	Child
P	Partner

Data received

Our work was based on the datasets received for the purpose of this exercise. We have not verified these inputs against original source documents except where stated.

Data sources and information used:

The following data files were received from Tayside Pension Fund on 30 April 2026:

- Spreadsheet titled, “Deferred Data Audit Info 20260428” for the deferred members
- Spreadsheet titled, “Dependant Data Audit Info 20260430” for the dependants
- Spreadsheet titled, “Pensioner Data Audit Info 20260430” for the pensioners

Summary of data checks performed (1 of 2)

This report has been prepared for, and is addressed to, the Scheme.

During our testing we have run the following tests on the data files provided. Unless stated otherwise, these tests have been ran for deferreds, pensioners and dependants.

The numbers in the report reflect the number of records with issues. There may be multiple issues on the same record and are therefore counted more than once in the aggregated numbers.

- Check that member ID is populated and unique
- Check that postcode is populated and valid
- Check that sex is populated and valid
- Check that marital status is populated (pensioner and deferred only)
- Check that total pre and post commutation pension and cash taken is populated and valid (pensioner only)
- Check that Date of Birth is populated and reasonable
- Check that Date of Joining Company is populated, valid and reasonable (pensioner and deferred only)
- Check that Date of Joining Scheme is populated, valid and reasonable (pensioner and deferred only)
- Check that Date of Leaving Scheme is populated, valid and reasonable (pensioner and deferred only)
- Check that Date of Retirement is populated, valid and reasonable (pensioner only)
- Check that state pension date is populated (pensioner only)
- Check that Date of Death is populated and valid (dependant only)
- Check that retirement type is populated and valid (pensioner only)
- Check that Initial AVC Pension and Current AVC Pension are populated, valid and consistent (pensioner only)
- Check that TV-in value and TV-in date are populated (deferred and pensioner only)
- Check that member contributions is populated (deferred only)

Summary of data checks performed (2 of 2)

This report has been prepared for, and is addressed to, the Scheme.

During our testing we have run the following tests on the data files provided. Unless stated otherwise, these tests have been ran for deferreds, pensioners and dependants.

- Check that the tranches at the valuation date are populated and valid (deferred and pensioner only)
- Check that the total pension at the valuation date is consistent with the tranches
- Check that spouse DoB is populated and valid (pensioner only)
- Check that total CSP at the valuation date is populated (pensioner only)
- Check that the CSP tranche is populated where a member's tranche is and vice versa (pensioner only)
- Check that the CSP tranche is valid (pensioner only)
- Check that final pensionable salary is populated (deferred only)
- Check that original member ID is populated (dependant only)
- Check that original member DoB is populated and valid (dependant only)
- Check that original member Date of Leaving Scheme is populated and valid (dependant only)
- Check if there are duplicates in the dataset
- Check that there are no categories containing an unreasonable number of repeated entries
- Check that the GMP tranches rounds to the statutory 52p if it is a GMP tranche (pensioner and dependant only)

Additional notes

Data not provided and therefore not tested:

Deferreds

- Adjustments or special benefits that have been made at or after Date of Leaving Scheme (for example, divorce debit, discretionary deferred increases, redundancy/ill health etc)
- Members' pension split into the relevant tranches at Date of Leaving
- Details on the guaranteed minimum pension (GMP) to be paid
- Details on contingent spouse data
- Members' normal retirement date
- Member AVC information

Pensioners

- Final pensionable salaries
- Members' pension split into the relevant tranches at Date of Leaving and Date of Retirement
- Details of any insured benefits, including details of the benefits insured vs full Scheme benefits, ability to restructure the insurance policy(ies), when the policy(ies) was taken out and if the policy(ies) are in the Trustee's name
- Adjustments or special benefits that have been made at or after retirement (for example, LEA, anti-franking step-up, divorce debit, discretionary increases in payment, redundancy/ill health etc)
- Consistency between the member's pension tranches at different accrual rates and the amount of CSP in each tranche

Dependants

- Original member service dates
- Original member pension split into the relevant tranches at Date of Death
- Original member AVC information

This page is intentionally left blank

5

Appendix 5 – Terms of Reference (ToR)

This page is intentionally left blank

Background and audit objective

Background

Ensuring high-quality data is fundamental to the effective management, governance, and administration of the pension scheme. Accurate, complete, and consistent data form the foundation upon which all key pension processes depend, - from calculating and paying member benefits to meeting statutory and regulatory reporting obligations. Reliable data enables administrators and trustees to deliver timely and correct benefits, maintain compliance with legislation, and make well-informed strategic decisions regarding funding, investment, and risk management.

Identifying and addressing data deficiencies at an early stage is essential to achieving operational efficiency and reducing the likelihood of costly errors or delays. Proactive data management, including regular audits, validation checks, and data cleansing exercises, supports smoother scheme administration and enhances the member experience by ensuring communications and benefits are accurate. In the long term, maintaining robust data standards helps preserve the integrity, transparency, and sustainability of the pension scheme, instilling confidence among members, employers, and regulators alike.

Audit objective

The objective of this review is to conduct a comprehensive data gap analysis of the Tayside Pension Fund ("the Scheme", or "TPF")'s data, assessing its internal consistency, completeness, and accuracy. This review is therefore essential to safeguard member interests and facilitate seamless execution of future scheme activities.

An estimated 15 audit days have been allocated for this work, on the basis that it will be primarily desk based, supported by targeted virtual or in person discussions and walkthroughs with key stakeholders, and that relevant documentation and evidence will be readily accessible.

Audit scope and approach

Scope

Our scope will consist of the following services in relation to review of the TPF's membership data quality for members:

- Obtain a copy of membership data and undertaking a data gap analysis on the Pension Scheme's data for internal consistency, completeness and accuracy for future scheme activity.
- A report to the Trustee setting out our results.

We will be using our Data Gap Analyser (DGA), an Alteryx workflow that applies approximately 800 tests to the data to assess internal consistency, completeness, and integrity, as well as to identify any potential outliers. In addition, the results will be uploaded to a Power BI dashboard, which enables interactive exploration and analysis of the findings.

These services are dependant on the following assumptions:

- The data provided is of sufficient quality to complete the data gap analysis, with no known material concerns.
- Where assumptions are required on the data to resolve any gaps, we would agree these with TPF Management and document them accordingly.
- We would also note the following additional points:
- We would not have any liability in respect of errors that are contained within the data provided to us.
- We would not be rectifying any benefits as part of this service if there are any errors found based on our DGA test outcome.
- We would not be responsible for arranging payments to members in respect of arrears, nor for managing any associated tax consequences associated with the arrears payments.

Limitations of scope and audit approach

Limitations of Scope

The scope of our review is intentionally focused and subject to the following limitations:

- No validation of source systems: Our work is limited to reviewing the membership data extract provided to us. We will not verify the completeness or accuracy of underlying source systems, data feeds, or historical data entry processes.
- No assessment of controls: The review does not include an evaluation of the Pension Scheme's data governance framework, operational controls, or IT controls relating to the capture, maintenance or transmission of member data.
- No reconciliation to actuarial or payroll records: We will not independently reconcile the membership data to actuarial records, payroll systems, AVC providers or third-party administrators beyond what is required for internal consistency checks.
- Internal consistency testing only: Our Data Gap Analyser (DGA) applies c.800 rules to assess internal consistency, completeness, integrity, and potential outliers. These tests do not confirm the real-world accuracy or validity of member attributes (e.g., correct dates of birth, correct salaries, correct benefit classifications).
- No judgement on benefit entitlements: The review will not assess whether individual member benefits have been calculated correctly or whether benefit entitlements comply with scheme rules or legislative requirements.
- No confirmation of data materiality or financial impact: While we will highlight gaps and anomalies, we will not quantify the financial or operational impact of any issues identified.
- Reliance on provided data: Our conclusions will rely on the accuracy and completeness of the data extract supplied. We will not independently verify whether all relevant members or fields have been included.
- Point-in-time review: The analysis reflects data quality at the point of extraction only and does not provide assurance over on going data maintenance processes or improvements.

Audit approach

Our audit approach is as follows:

- Our advice will take the form of a written report, verbal discussions, attendance at meetings and updated data files.
- We will be performing a substantive audit focused on the completeness and consistency of the data. Exceptions will be discussed with management to understand whether they were caused by control failures. Recommendations will be provided to management to investigate the root causes and implement remedial actions where necessary.

PricewaterhouseCoopers LLP is a limited liability partnership registered in England with registered number OC303525. The registered office of PricewaterhouseCoopers LLP is 1 Embankment Place, London WC2N 6RH. PricewaterhouseCoopers LLP is authorised and regulated by the Financial Conduct Authority for designated investment business and the Solicitors Regulation Authority for the provision of regulated legal services.

This document has been prepared only for Tayside Pension Fund (the “Scheme”) and solely for the purpose and on the terms agreed with the Scheme in our terms of reference dated 31 March 2026. We accept no liability (including for negligence) to anyone else in connection with this document, and it may not be provided to anyone else.

© 2026 PricewaterhouseCoopers LLP. All rights reserved. ‘PwC’ refers to the UK member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.