ITEM No …10…..…..

REPORT TO: **PENSION SUB-COMMITTEE OF THE POLICY & RESOURCES COMMITTEE & PENSION BOARD – 21 MARCH 2022**

REPORT ON: **TAYSIDE PENSION FUND INTERNAL AUDIT REPORT – RISK MANAGEMENT & REGULATORY COMPLIANCE REVIEW**

REPORT BY: **EXECUTIVE DIRECTOR OF CORPORATE SERVICES**

REPORT NO: **87-2022**

1 PURPOSE OF REPORT

To submit to the Sub-Committee the Audit Report prepared by the Fund's Internal Auditor, PricewaterhouseCoopers (PwC).

2 RECOMMENDATIONS

The Sub-Committee is asked to note the content of the report on the audit exercise undertaken, and to approve the management response.

3 FINANCIAL IMPLICATIONS

None.

4 MAIN TEXT

4.1 Internal Audit Report - Risk Management and Regulatory Compliance Review (Appendix A)

The report details the review of the design and operating effectiveness of the risk management and regulatory compliance processes and procedures in place, and the risk management framework that allows the Pension Board and Sub-Committee to identify, evaluate and record and monitor both the risks and the internal controls that have been established to manage them.

4.2 PwC have rated the control environment as satisfactory with exceptions, and medium risk. Further details are included in Appendix A of their report. PwC classify medium risk as that a finding could have moderate impact on operational performance, reputation, financial impact, or regulatory breach.

4.3 The findings and recommendations of the audit have been discussed with management and their responses are contained within the reports. The implementation of the agreed management actions will be monitored, with progress being reported to the Sub-Committee in due course.

5 POLICY IMPLICATIONS

This report has been screened for any policy implications in respect of Sustainability, Strategic Environmental Assessment, Anti-Poverty, Equality Impact Assessment and Risk Management. There are no major issues.

6 CONSULTATIONS

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

7 BACKGROUND PAPERS

None

ROBERT EMMOTT
EXECUTIVE DIRECTOR OF CORPORATE SERVICES **11 MARCH 2022**

Tayside Pension Fund Internal Audit Report

Risk Management and Regulatory Compliance review

Tayside Pension Fund
Final
February 2022

Click to launch

pwc

Contents

Distribution list

For action:
Senior Manager Financial Services

For information:
Pension Board & Pension Sub-Committee
Executive Director Corporate Services
Head of Corporate Finance

Executive summary

Report classification

Satisfactory with exceptions (7 points)

Total number of findings

	Critical	High	Medium	Low	Advisory
Control design	-	-	2	1	-
Operating effectiveness	-	-	-	-	-
Total	**-**	**-**	**2**	**1**	-

Our review considered the design and operating effectiveness of the risk management and regulatory compliance processes and procedures in place at Tayside Pension Fund (TPF). We reviewed the aspects of the risk management framework that allow the Pension Board and Sub-Committee to identify, evaluate and record risks and monitor the internal controls that have been established to manage those risks. This included the processes and controls which ensure the delivery of the risk management framework. The detailed scope of this review can be found in Appendix B.

A summary of our findings noted during our review are as follows:

- **Risk register requires improvements to enhance risk monitoring (Medium).** We noted opportunities for further enhancement of the risk register to ensure the risk management monitoring procedures are appropriate, for example, the current risk register format is not comprehensive enough as it does not include information which helps to improve the risk monitoring process.
- **No risk appetite statements and risk assessment mechanism (Medium).** From our review, we noted that TPF does not have a risk assessment matrix and risk appetite statement of its own, as it uses the ones for the Dundee City Council. Without an appropriate risk assessment matrix and risk appetite statement which are tailored for TPF's specific risks, there is a risk that wrong decisions could be made which could prevent TPF from achieving its strategic objectives.
- **Training and Awareness (Low).** We noted that TPF does not currently maintain a risk management training plan for staff with risk responsibilities or an awareness program for the embedding of risk across the organisation.

Our detailed findings are on pages 2 to 5 of this report. We have also included further insights on some aspects of risk management in Appendix D of this report .

Current year findings

1 Risk register requires improvements to enhance risk monitoring

Control design

Finding rating

Rating	Medium

Finding and root cause

The risk register is the main repository for monitoring the risks at TPF. Risks are assessed using a common impact and likelihood criteria to assess the inherent and current (residual) scores, which is subsequently plotted on a heat map (Red, Amber, Green) to ascertain risk movement between the risk ratings. The TPF risk register is downloaded (quarterly) from the Pentana system and it is reviewed by the head of finance and executive director of corporate services, who is also the s95 officer. The reviewed risk register then goes to the quarterly Joint meeting (Pension Committee and Pensions board) for the final review and approval.

From the work performed, the following opportunities for further enhancement of the risk register were identified:

- **Risk descriptions and missing information** – We noted risk descriptions which are not sufficiently detailed. Capturing the primary cause, event and consequence(s) of a risk will allow TPF to more accurately assess risks and determine the most appropriate controls or mitigating actions required to manage them more effectively. See appendix D for the detail regarding the cause, event and consequence risk description elements. Furthermore, we noted 8 risks with blank columns on the risk register.
- **Completeness of risks** – We noted that some risks that could affect the achievement of strategic or operational objectives for TPF were not included on the register, for example,

i. The risk that TPF would not be prepared to implement the new Pensions dashboards when they are introduced. According to a survey conducted by The Pensions Regulator's (TPR's) Public Service Pension Scheme (PSPS) Governance and Administration which was completed by representatives of 193 public service pension schemes out of the existing entirety of 206, only 40% of the schemes agreed that they would be able to deal with any administrative demands (of the pensions dashboard) involved and only 9% believed that dashboards would be easy for their scheme to implement. As such, TPF should include the pensions dashboard as a risk on their register to ensure that the necessary controls are put in place to mitigate the risk.

ii. Risks relating to the use of third parties to support operations, e.g. poor due diligence and selection processes, failure of a supplier to follow agreed upon procedures, financial failure of supplier resulting in inability to deliver service.

iii. Failure to comply with governance best practice (eg TPR Code of Practice (CoP) 14, Good Governance project outcomes and the new draft consolidated CoP)

iv. Poor quality service to members and employers.

v. No risks in respect to McCloud, GMP or the Lloyds judgement.

vi. We note that risk 13, *Failure to hold personal data securely (incorporating Cyber Crime),* has a lower inherent risk rating to what we would typically see elsewhere. In addition, we note the resulting residual risk is then higher than the inherent risk which appears misaligned. Through discussions with management we note that all the risk ratings require review.

Current year findings

1 Risk register requires improvements to enhance risk monitoring

Control design

Finding rating

Rating	Medium

Potential implications

If the suggested enhancements to the risk register report are not implemented, the risk register approach would not be focused, efficient and streamlined, resulting in the risk of insufficient risk monitoring procedures and exposing TPF to unnecessary risk.

Management action plan

We will review the risk register report and make the suggested changes which include:

- Update the current risk descriptions to use cause, event and consequence format, that are specific to TPF.
- Develop a systematic process in order to help identify risks to ensure that the risk register contains all the risks that TPF is exposed to.

TPF will consider conducting risk identification and assessment workshops in order to help embed a productive risk management culture.

Responsible person/title: Tracey Russell

Target date: 31 March 2022

Current year findings

2 No risk appetite statement and risk assessment mechanism

Control design

Finding rating

Rating	Medium

Finding and root cause

TPF does not have a risk assessment matrix and risk appetite statement of its own, as it uses the ones for the Dundee City Council. Risk assessment and determining risk appetite is key to achieving effective risk management and is essential to support decision making which supports how risks can ultimately be addressed. Risk appetite provides a framework which enables an organisation to make informed management decisions. By defining both optimal and tolerable positions, an organisation clearly sets out both the target and acceptable position in the pursuit of its strategic objectives. TPF should develop its own processes and procedures as there is no one-size-fits-all solution for risk assessment and risk appetite statements. For example using the same amount to assess/score the risks for both TPF and the Council could produce an inappropriate assessment as an amount could be material to TPF but might not be material to the Council. We have included further insight on risk appetite statement and risk assessment mechanism within appendix D.

Potential implications

Without an appropriate risk assessment matrix and risk appetite statements which are tailored for TPF's specific risks, there is a risk that wrong decisions could be made which could prevent TPF from achieving its strategic objectives.

Management action plan

- To develop a risk assessment matrix and risk appetite statement which are specific to TPF.
- The risk appetite statement will be linked to the risk scoring matrix in a way which would allow identification of instances where residual risk is above the set risk appetite level.

Responsible person/title: Tracey Russell

Target date: 31 March 2022

Current year findings

3 Lack of risk training and awareness

Control design

Finding and root cause

Ongoing risk management training programmes are important to ensure all employees understand the value and importance of risk management, and what is required of them. TPF does not currently maintain a risk management training plan for staff with risk responsibilities or an awareness program for the embedding of risk across the organisation. We understand from our discussion with management that a training program is currently being developed by the Council with training and education that will be rolled out to the relevant staff, however this may not necessarily address the needs for the TPF team.

Potential implications

There is a risk that TPF staff are not aware of the risk strategy and key risks of the organisation thus risk approach/awareness would not be at the desired level of management. The risk owners might not be able to effectively carry out their roles and responsibilities due to a lack of sufficient guidance and training.

Finding rating

Rating	Low

Management action plan

- To develop an awareness and training program that will be reviewed, signed off, and monitored for implementation by the Pension Committee and Pensions board.
- Training log will be maintained to monitor the training program

TPF should consider conducting risk identification and assessment workshops in order to help embed a productive risk management culture.

Responsible person/title: Tracey Russell

Target date: 31 March 2022

Appendices

Appendix A: Basis of our classifications

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.

Appendix A: Basis of our classifications

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
- **Minor** impact on the reputation of the organisation.

Advisory

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
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 – 39 points
Unsatisfactory	40 points and over

Appendix B: Terms of reference
Background and audit objectives

This review is being undertaken as part of the 2021/2022 internal audit plan, which was approved by the Pension Sub-Committee on 8th March 2021.

Background

Tayside Pension Fund has been administered by Dundee City Council since 1st April 1996. It is part of the Local Government Pension Scheme (LGPS), which is a statutory scheme established under the primary legislations of the Superannuation act 1972 and Public Service Pensions Act 2013.

As at 31st March 2021, Tayside Pension Fund had investment assets of £4.85 billion, and a membership of over 51,000 across 45 participating employers. These participating employers include 3 local authorities, as well as their subsidiary companies and contractors; a number of universities and colleges; and a range of organisations with funding or service links to local government.

There are approximately 100 LGPS funds in the UK, with 11 of these in Scotland. Tayside is the 4th largest of the 11 Scottish LGPS funds in asset size. The LGPS is a multi-employer defined benefit scheme, whose benefits up until 31st March 2015 was based upon final salary. Since this date, benefits are based upon career average.

The rules by which the LGPS scheme operates by are set out in the Local Government Pension Scheme (Scotland) Regulations which are Scottish Statutory Instruments (SSIs). Separate regulations set out scheme benefits, investment and governance requirements

An audit of Risk Management and Regulatory Compliance is included in the 2021/2022 Internal Audit plan approved by the Pension Sub-Committee on 8th March 2021. This audit will focus on reviewing the process in place for evaluating risks and establishing adequate internal controls. This will include an assessment of the risk register, and the process of its review and challenge. We will also look to understand how the Pension Board and Sub-Committee obtains comfort over compliance arrangements and the controls in place to identify and sufficiently mitigate applicable regulatory changes.

Audit Objectives

Review the aspects of the risk management framework that allow the Pension Board and Sub-Committee to:

- Identify, evaluate and record risks, in order to identify those that are critical to the scheme and consider the impact and likelihood of a risk materialising.
- Monitor the internal controls that have been established to manage those risks.
- Obtain comfort over compliance arrangements, and the controls in place to identify and sufficiently mitigate applicable regulatory changes.

Appendix B: Terms of reference

Audit scope and approach

Scope

We will review the design and operating effectiveness of key controls relating to risk management during the 12 month period to 31st August 2021.

The processes, risks and related control objectives included in this review are:

Process	Objectives	Risks
Risk Management Framework Design	To review the aspects of the risk management framework that allow the Pension Board and Sub-Committee to identify, evaluate and record risks and monitor the internal controls that have been established to manage those risks. This will include a review of: • Risk management policy, processes and supporting guidance documentation • Risk roles, associated responsibilities and relevant terms of reference. • Risk identification and assessment activities, which will specifically include regulatory and compliance risk.	• Lack of an appropriate risk management framework could result in inadequate identification and appropriate mitigation of risks which may impact on the achievement of the Fund's objectives.
Risk Management Delivery	To review the processes and controls which ensure the delivery of the risk management framework. This will include a review of: • Risk reporting (e.g. Risk management information is reported to the Pension Board and/or relevant committee on a regular basis) • Risk registers (quality and completeness of recorded information) • Risk analysis outputs and monitoring of risk response, which will specifically include regulatory and compliance risk.	• Lack of appropriate risk management delivery processes could results in inadequate identification and appropriate mitigation of risks which may impact on the achievement of the Fund's objectives. • Insufficient Pension Board and Sub-Committee operating arrangements could lead to poor decision making and risk management.

Appendix B: Terms of reference

Audit scope and approach

Limitations of scope

This audit will focus on assessing the design adequacy and operating effectiveness of the risk management framework and risk management delivery of Tayside Pension Fund, specifically the scope is limited to the objectives noted above.

Audit approach

Our audit approach is as follows:

- Obtain an understanding of the risk management framework through discussions with key personnel and review of the risk management policy, processes and supporting guidance documentation.
- Review risk roles, associated responsibilities and relevant terms of reference.
- Identify the key processes and controls which ensure the delivery of risk management.
- Evaluate the design of the key processes and controls in place.
- Test the operating effectiveness of the key processes and controls in place.

Appendix 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 for the period specified 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 endeavour to plan our work so that we have a reasonable expectation of detecting significant control weaknesses and, if detected, we carry 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.

Appendix D: Further insight – risk description

*Risk description elements:

Cause	Event	Consequence(s)
The sources of the risk event, the reason why the risk could happen	Actions, incidents, or occurrences that arise from a cause that could have an affect on the achievement of objectives	Possible consequences arising from the Risk Event that affect the achievement of objectives

Risk description:

- **Cause** [Y], or "from any cause whatsoever" if looking principally at impact
- Description of **Event** [X]
- **Consequence(s)** – impact on the pension scheme [Z] – use and/or so that you can approximate the value of the impact

General case

"There is a risk that [X might occur] as a result of [Y] resulting in [Z]."

Appendix D: Further insight – risk appetite

Risk appetite is a matter of judgement based on each scheme's specific circumstances and objectives. There is no one-size-fits-all solution. Guiding principles to keep in mind when developing risk appetite statements and metrics include but are not limited to the following:

Simplicity	▪ Use simple, non-technical language
Practicality focused	▪ Not developed for every risk or decision
Linked to strategy	▪ Articulate the desired risk taking approach in relation to delivering relevant strategic objectives and protecting core values
Reflect opportunity	▪ Not be seen as purely a limitation on risk taking and exposure - an articulation of the Board's desired risk and reward balance
Measurable	▪ Incorporate metrics and thresholds to support measurability and help prevent breaches

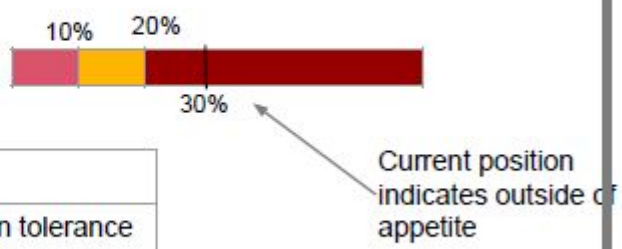
Key questions to consider:

- Strategy
  - Are we taking enough risk?
  - Are we taking too much?
  - Zero appetite – exit?
- Key investment / major change decisions
  - What are the rewards?
  - What risks are attached and should we take them?
  - What opportunities are we missing if we don't?
  - Are we being too aggressive / too conservative?
  - What is the risk/reward balance?
  - What mitigations do we need in place to be comfortable?

Simplified approach to risk appetite could be focused on the KRI thresholds rather than a qualitative statement

Quality of member service

% increase in member complaints within 1 month period



Appendix D: Further insight – risk assessment

An example of risk assessment parameters – severity ratings :

Business area/risk category	Impact - Severity rating				
	1 Minimal	2 Minor	3 Moderate	4 Major	5 Catastrophic
Financial (unanticipated financial loss)	Less than £X k	£X k -> £Y k	£Y k -> £Z m	£Z m -> £A m	Over £A m
Operational (interruption)	Piecemeal interruption less than 1 day	Broad interruption less than 1 day	1 -> 3 days	3 -> 15 days	Over 15 days' interruption
Legal, Regulatory and Compliance	No interest from regulatory authority.	Regulatory authority requests explanation with ongoing updates	Regulatory authority launches informal investigation i.e. written request	Regulatory authority launches formal investigation with potential for fine	Potential for significant fine or requiring revision of operating model.
Customer (Industry) Reputation	Little or no impact on reputation	Some impact on reputation with principals	Principal monitors scheme due to the level of distrust	Loss of trust means that principals seek guidance externally	Fundamental change in relationship with principals
People	Staff turnover higher than expected with little or no impact on operations Employee injury requiring medical aid < 3 days sick leave	Staff turnover significant, impacting on efficiency and effectiveness Employee injury requiring medical aid >3 days sick leave Third party injury	Limited loss of key skills (1/2 individuals) Injury to employee /third party requiring hospitalisation (>24 hrs) or permanent disablement	Loss of multiple skills or loss of mission-critical individual Single employee/third party fatality Multiple disabling injuries to employees/third party	Irrecoverable loss of multiple key skills Multiple employee/third party fatalities
Strategy	Could have a minor impact on a functional objective and no impact on the overall strategy	Could have a major impact on one or more functional objectives, but no impact on the overall strategy	Could have a major impact on one or more functional objectives or some limited impact on overall strategy	Significant impact on ability to deliver a strategic objective	Scheme unable to meet multiple strategic objectives

Appendix D: Further insight – risk reporting

Below provides a high level overview of risk reporting tips.

Focus

Reporting should identify specific rather than generic risks, and tie them to the organisation's individual circumstances. Consider:

- Is the risk clearly explained?
- Is the cause(s) of the risk discussed?
- How does the risk relate to the business model and/or strategy?

1

Relevance/Materiality

The organisation's estimate of how likely each risk is to materialise and how and when its consequences would be felt, should be clear. Consider:

- Would the consequence(s) be direct and/or indirect and what would they be?
- Would the consequence(s) be short-term, medium-term or long-term?
- Which stakeholders are interested and/or affected?

2

Status

What is being done about the risk in terms of active management or other mitigation? Specifically:

- Is the risk currently within the risk appetite parameters?
- Are there any failings or weaknesses of risk management or internal control in connection with the risk? Are they significant?
- What has changed in relation to the assessment and management of the risk since the last reporting period, and what is expected to change going forward?

3

Remember to consider how stakeholder interests may increase the impact/likelihood of your current and emerging risk profile. By incorporating stakeholder views and agendas into the risk management process you may also get early warning of incoming risks before they fully materialise.

Thank you

pwc.co.uk

190219-133533-JS-OS