Deloitte.

Shetland Islands Council

Shetland Islands Council Pension Fund

Planning report to the Pension Fund Committee on the 2020/21 audit

Issued 26 January 2021 for the meeting on 11 February 2021

Contents

Executive introduction

The key messages in this report:

We have pleasure in presenting our Planning Report to the Pension Fund Committee for the 2020/21 audit of Shetland Islands Council Pension Fund ('the Fund'). We would like to draw your attention to the key messages of this paper:

Audit quality is our number one priority.

We plan our audit to focus on audit quality and have set the following audit quality objectives for this audit:

A **robust** challenge of the key judgements taken in the preparation of the Annual Accounts.

A strong **understanding** of your internal control environment.

A **well planned** and delivered audit that raises findings early with those charged with governance.

Fund Changes

Following discussions with the Fund's finance team, we have not identified any significant changes to the Fund during the year. We will continue to liaise with the finance team to identify any changes between the date of this report and the Fund's year end, and will update our audit plan accordingly should any occur.

There have been no significant regulatory changes to the accounting of the Fund in the current year. The Code of Practice on Local Authority Accounting in the United Kingdom 2020/21 ("the 2020/21 Code") applies in the current year.

Significant audit risks

As in the prior year, we have identified management override of controls as our significant audit risk. Auditing standards require us to assume that management override of controls is an audit risk for all of our audits.

Further details of this significant risk, including our proposed testing can be found on page 13.

Whilst the accuracy and timeliness of contributions and completeness of investment transactions and valuation of pooled property funds have not been assessed as significant risks, they have been assessed as audit focus areas as outlined on pages 15 and 16.

Audit Quality

Our audit approach is tailored to providing the Pension Fund Committee with an audit which is designed to provide assurance and insight over the Fund control environment.

We plan and deliver an audit that raises findings early with those charged with governance. This is underpinned by mutually agreed timetables, detailed audit request lists and frequent communications with management and the Pension Fund Committee.

Executive introduction (continued)

The key messages in this report:

Our response to the audit quality objectives in respect of the Fund are detailed below:

Our audit quality is managed by using dedicated pension scheme audit specialists. This structure allows us to challenge key judgements taken in the preparation of the Annual Accounts.

Audit dimensions

The Code of Audit Practice sets out four audit dimensions which set a common framework for all public sector audits in Scotland. Our audit work will consider how the Fund is addressing these and we will report our conclusions in our annual report to the Members and Controller of Audit in September 2021. In particular, our work will focus on:

- ***Financial sustainability –*** we will monitor the Fund's actions in respect of its medium and longer term financial plan to assess whether short term financial balance can be achieved, whether there is a long-term financial strategy and if the investment strategy is effective.
- ***Financial management –*** we will review the budget and monitoring reports of the Fund during the year to assess whether financial management and budget setting is effective.
- ***Governance and transparency –*** from our review of the Fund's Pension Fund Committee papers and attendance at Pension Fund Committee meetings, we will assess the effectiveness and scrutiny of governance arrangements. We will also share best practice examples, where it is deemed appropriate.
- ***Value for money –*** we will gain an understanding of the Fund's self-evaluation arrangements to assess how it demonstrated value for money in the use of resources and the linkage between money spent and outputs and outcomes delivered.

Pat Kenny
Audit Director

Responsibilities of the Pension Fund Committee

Helping you fulfil your responsibilities

The primary purpose of the Auditor's interaction with the Pension Fund Committee:

- To communicate audit scope
- To provide timely and relevant observations
- To provide additional information to help you fulfil your broader responsibilities
- Provide assurance over the Annual Accounts

We use this symbol to highlight areas of our audit where the Pension Fund Committee needs to focus attention.

As a result of regulatory change in recent years, the role of the Pension Fund Committee has significantly expanded. We set out here a summary of the core areas of Pension Fund Committee responsibility to provide a reference in respect of these broader responsibilities and highlight throughout the document where there is key information which helps those charged with governance in fulfilling their remit.

Integrity of reporting

- Review of external audit findings, key judgements, level of misstatements.
- Assess the quality of the Fund advisors where activities have been delegated by the Pension Fund Committee.
- Assess the completeness of disclosures, including consistency with disclosures required under the Code of Practice on local authority accounting in the UK.

Oversight of external audit

- At the start of each annual audit cycle, ensure the scope of the external audit is appropriate.
- Implement a policy on the engagement of the external auditor to supply non-audit services.

Internal controls and risk

- Review the internal control reports and risk management systems for Fund advisors.
- Explain what actions have been, or are being taken to remedy any significant failings or weaknesses.

Oversight of internal audit

- Consider annually whether there is a need for an internal audit function and any testing to be performed over pension activities.

Whistle-blowing and fraud

- Ensure that appropriate arrangements are in place for the proportionate and independent investigation of any concerns that are raised by staff in connection with improprieties.

Timing of the audit

Continuous communication and reporting

As the audit plan is executed throughout the year, the results will be analysed continuously and conclusions (preliminary and otherwise) will be drawn and initial comments from the final visit will be shared with management as required. The following sets out the expected timing of our reporting to and communication with you.

Planning	Year end fieldwork	Reporting
• Planning meetings • Discussion of fraud risk assessment • Audit team issues planning report to the Pension Fund Committee (February 2021)	• Audit of Annual Accounts • Test the design and implementation of the control environment at the Fund • Review of investment confirmations and fair value testing of investments • Year end audit field work	• Issue Annual Audit Report to the Pension Fund Committee and the Controller of Audit and presentation of report and attendance at the Pension Fund Committee meeting • Audit de-brief on the 2020/21 audit • Reporting of significant control deficiencies • Signing audit reports in respect of the Annual Accounts • Issue audit report and submission of the audited Annual Accounts to Audit Scotland
2021 Audit Plan	Continuous reporting to Management	Final Report to the Pension Fund Committee and any additional reporting as required
February/March 2021	July/ August 2021	September 2021

Ongoing communication and weekly calls during the year end fieldwork phase

Materiality

Our Approach to Materiality

Basis of our materiality benchmark

- We have estimated materiality for our opinion on the individual financial statements as £4,607k, based on professional judgement, the requirement of auditing standards and the prior year net assets of the Fund.
- We have used 1% of Fund net assets as the benchmark for determining our materiality levels.

The basis for our materiality calculations is the same as the previous year.

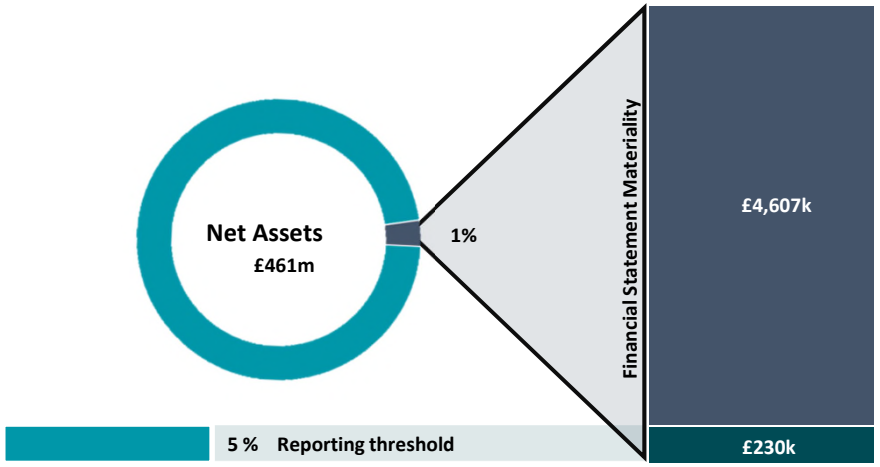
Materiality Calculation

We set performance materiality as a percentage of materiality (typically 70%) to reduce the probability that, in aggregate, uncorrected and undetected misstatements exceed materiality. We determine performance materiality, with reference to factors such as the quality of the control environment and the historical error rate. Where we are unable to rely on controls, we may use a lower level of performance materiality. It is performance materiality that is used in the determination of our audit samples.

Although materiality is the judgement of the audit director, the Pension Fund Committee must be satisfied the level of materiality chosen is appropriate for the scope of the audit.

Reporting to those charged with governance

- We will report to you all misstatements found in excess of 5% of financial statement materiality. We will report to you misstatements below this threshold if we consider them to be material by nature.
- We will determine current year materiality figure and reporting to those charged with governance figure for the Fund on receipt of the draft 2020/21 Annual Accounts.



Scope of work and approach

Our key areas of responsibility under the Code of Audit Practice

Core audit

Our core audit work as defined by Audit Scotland comprises:

- Providing the **Independent Auditor's Report** on the Annual Accounts
- Providing the **annual report** on the audit addressed to the Pension Fund Committee;
- Communicating **audit plans** to the Pension Fund Committee;
- Providing **reports to management**, as appropriate, in respect of the auditor's responsibilities in the Code;
- Identifying **significant matters arising from the audit**, alert the Controller of Audit and support Audit Scotland in producing statutory reports as required; and
- Undertaking work requested by Audit Scotland or local performance audit work.

Wider scope requirements

The Code of Audit Practice sets out four audit dimensions which set a common framework for all public sector audits in Scotland:

- **Financial sustainability –** looking forward to the medium and longer term to consider whether the Fund is planning effectively to continue to deliver its services or the way in which they should be delivered.
- **Financial management –** financial capacity, sound budgetary processes and whether the control environment and internal controls are operating effectively.
- **Governance and transparency –** the effectiveness of scrutiny and governance arrangements, leadership and decision making, and transparent reporting of financial and performance information.
- **Value for money –** using resources effectively and continually improving services.

Scoping

Significant Risk + Areas of Audit Focus Dashboard

Risk Identified	Material Balance	Management Judgement	Proposed Approach	Fraud Risk	Further Details
Significant Risk Management override of controls	✗	⚠	**D&I**	✓	Pg. 13
Other Focus Area Completeness of investment transactions and valuation of pooled property funds	✓	⚠	**D&I + OE**	✗	Pg. 15
Other Focus Area Accuracy and timeliness of contributions	✗	⚠	**D&I**	✗	Pg. 16

Significant Risk		Low levels of management judgment/complexity		**D&I**	Design and Implementation
Other area of audit focus		Medium levels of management judgement/complexity		**OE**	Operating Effectiveness
		High degree of management judgement/complexity			

Scoping (continued)

Significant Account Balances

Annual Accounts and audit scope coverage

Our principal audit objective is to obtain sufficient, relevant and reliable audit evidence to enable us to express an opinion on the Fund's Annual Accounts for the year ending 31 March 2021. Our audit work will be performed in accordance with our framework agreement, signed on 31 May 2016.

In addition to forming these opinions, we will also report to the Pension Fund Committee on:

- A summary of control weaknesses that we identify; and
- Significant audit findings, including commentary on key accounting judgments and disclosures.

In putting together this Report we have sought to:

- Plan our audit effort to focus on areas of risk. We have identified key areas of risk from our work to date and our knowledge of the Fund and your industry and planned appropriate audit responses; and
- Document our approach to the resolution of these risk areas such that they can be reported and acted upon promptly.

In reaching our opinions, it is necessary to determine whether the Annual Accounts comply with applicable accounting standards and legislation. We will conduct our audit in accordance with International Standards on Auditing (UK) ("ISA (UK)") and Practice Note 15 'the audit of occupational pension schemes in the United Kingdom'.

We consider a number of factors when deciding on the significant audit risks. These factors include:

- The significant risks and uncertainties previously reported in the Annual Accounts;
- The critical accounting estimates previously reported in the Annual Accounts;
- The disclosures made by the Pension Fund Committee in their previous Pension Fund Committee report;
- Our assessment of materiality; and
- The changes that have occurred in the Fund year and the environment it operates in since the last Annual Accounts.

Pages 9 and 11 summarise our scoping rationale for account balances and significant risks.

Scoping (continued)

Summary of Account Balances

Scoping Key Account Balances

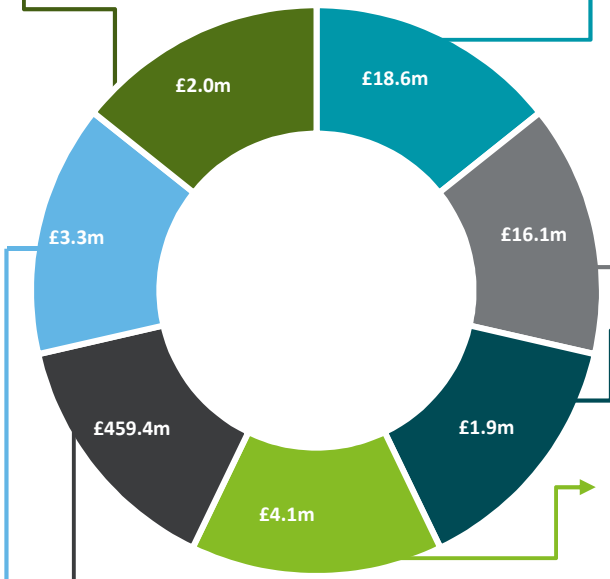
We have considered each of the Fund's significant account balances (based on the 31 March 2020 signed Annual Accounts).

For each balance, we explain the basis on which we have determined whether or not it will be a key audit matter and provide commentary.

We will report factually on the key audit matters that have the biggest impact on the audit.

We will explain why the matter is relevant within the specific circumstances of the Fund and clearly document the specific procedures we will perform to address the key audit matter.

These areas are considered in more detail on pages 13 to 16.



Current liabilities
We have not referred to this risk in our report to the Pension Fund Committee because the balance is not material.

Contributions
This is a material balance. We have considered the risk in respect of accuracy as well as timeliness on page 16.

Benefits and Transfers
Benefits payable and transfers consists of material pensions payable and transfers out. We have not referred to this risk in our report to the Pension Fund Committee because the balance is considered routine in nature.

Administration and Investment Management Expenses
We have not referred to this risk in our report to the Pension Fund Committee because the balance is not material.

Investment income
This is a material balance and will be subject to substantive audit testing. However, we have not referred to this risk in our report to the Pension Fund Committee because the balance is considered routine in nature and is readily verifiable to independently obtained third party investment manager and custodian reports.

Current assets
We have not referred to this risk in our report to the Pension Fund Committee because the balance is not material.

Investments
Due to it's significance, we disaggregate the balance into categories of investments. This is a highly material balance. The risk in respect of completeness of investment transactions and valuation of pooled property funds is discussed on page 15.

We will report control observations and other findings in our final report to the Pension Fund Committee on work performed on other account balances.

Significant audit risk

Significant risk

Management override of controls

Risk identified

In accordance with ISA 240 (UK) management override is always a significant risk for financial statement audits. The primary risk areas surrounding the management override of internal controls are over the processing of journal entries and the key assumptions and estimates made by management.

Response of those charged with governance

The Pension Fund Committee does not have access to the Fund accounting system and does not process any journals in respect of the Fund.

The financial reporting process in place has an adequate level of segregation of duties.

Deloitte response to significant risk identified

In order to address the significant risk our audit procedures will consist of the following:

- Using data analytics in our journals testing to interrogate 100% of journals posted across the Fund and to identify journals or audit interest for substantive testing;
- Making inquiries of individuals involved in the financial reporting process about inappropriate or unusual activity relating to the processing of journal entries and other adjustments;
- Performing a walkthrough of the financial reporting process to identify the controls over journal entries and other adjustments posted in the preparation of the Annual Accounts;
- Reviewing the accounting estimates for bias, such as year-end creditor and debtor postings and the valuation of unlisted investments, that could result in material misstatement due to fraud, including whether any differences between estimates best supported by evidence and those in the Annual Accounts, even if individually reasonable, indicate a possible bias on the part of management;
- Ensuring that there is an appropriate level of segregation of duties over processing journal entries to the Annual Accounts throughout the year;
- Testing the design and implementation of controls around the investment and disinvestment of cash during the year; and
- Making enquiries of management in relation to the identification of related parties.


Audit focus
areas

Audit focus areas

Completeness of investment transactions and valuation of pooled property funds

Risk identified

The Fund holds a large and highly material portfolio of investments, which is diversified with several investment managers. As a result of this we consider the completeness of these investments to be an area of audit focus.

The Fund holds investments primarily in pooled funds, pooled property unit trusts and fixed income unit trusts with a range of investment managers. Due to the continuing uncertainty as a result of COVID-19, we will pay particular focus to the pooled property funds.

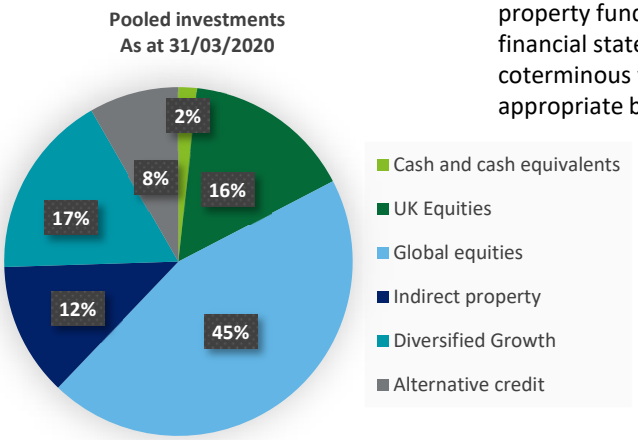
Response of those charged with governance

The Fund appoints various investment managers and Northern Trust as custodian for these investments. These parties have strong control environments in place.

Deloitte response to risk identified

In order to address this area of audit focus, we will perform the following audit procedures:

- Review the design and implementation and operating effectiveness of key controls over the valuation of investments by obtaining the investment manager and custodian internal controls reports and evaluating the implications for our audit of any exceptions noted;
- Independently request confirmations from all investment managers and the global custodian for balances held per the Annual Accounts;
- Agree year end valuations, sales proceeds and purchases in the Annual Accounts to the reports received directly from the investment managers;
- Perform a full unit reconciliation of investments held during the year;
- Perform valuation testing by using a range of techniques depending on the type of investment. For the pooled property funds, we will obtain audited financial statements and assess the year end price against the audited financial statements, and benchmark movements where the date of the audited financial statements is not coterminous with the Fund's financial year. We will consult with our Deloitte Real Estate department about the appropriate benchmarks to use.



Audit focus areas

Accuracy and timeliness of contributions

Risk identified

The correct deduction and timely payment of contributions depends on system-based processing of membership data and salary details, together with a robust internal controls framework. Errors in processing contributions can lead to issues such as non-compliance with the Local Government Pension Scheme Regulations 2014 ("LGPS Regulations") and the recommendations of the actuary, and deducting incorrect amounts from the active members' payroll, which can be costly to rectify and cause reputational damage.

In addition, while no opinion is issued on timely payment of contributions, it remains an area of focus, as LGPS Regulations stipulate due dates for payment. Late payments could cause reputational damage.

Response of those charged with governance	Deloitte response to risk identified
The administration team monitors the due dates of contributions and that the correct amounts are received into the Fund bank account to ensure that payments are in accordance with the recommendations of the actuary. Employers must also complete a contributions return confirming that the contributions paid during the year are accurate and complete.	In order to address this area of audit focus, we will perform the following audit procedures: • Review the design and implementation of key controls over the contribution process; • Perform an analytical review of the employer and employee normal contributions received in the year, basing our expectation on the prior year audited balance, adjusted for the movement in active member numbers, contribution rate changes and any average pay rise awarded in the year; • For a sample of active members, we will recalculate individual contribution deductions to ensure these are being calculated in accordance with the rates stipulated in the LGPS Regulations for employee contributions and the recommendations of the actuary for employer contributions; • Test that the correct definition of pensionable salary is being used per the LGPS Regulations to calculate contribution deductions; • Test the reconciliation of the total number of active members between the membership records and the employer payroll records; and • For a sample of monthly contributions paid, check that they have been paid within the due dates per the LGPS Regulations.


Wider scope
requirements

Wider Scope Requirements

Audit Dimensions

The Code of Audit Practice sets out four audit dimensions which set a common framework for all public sector audits in Scotland. We will consider how the Fund addresses these areas, including any risks to their achievement, as part of our audit work as follows:

Audit dimension	Areas to be considered	Impact on the 2020/21 Audit
Financial sustainability looks forward to the medium and longer term to consider whether the Fund is planning effectively to continue to deliver its services or the way in which they should be delivered.	• The financial planning systems in place across the shorter and longer terms. • The arrangements to address any identified funding gaps. • The affordability and effectiveness of funding and investment decisions made.	We will review arrangements and financial planning systems in place by the Fund to ensure that its services can continue to be delivered. This will include a review of the latest actuarial valuation of the Fund and the plans in place to reduce the deficit over the shorter and medium term. In addition, we will review the funding policy as set out in the Shetland Islands Council Pension Fund Investment Strategy, which aims to secure the long term solvency of the Fund, so that there are sufficient funds available to meet all benefits as they fall due. **Audit Risk:** The Fund's investment strategy is inconsistent with the long term solvency of the Fund. We have not identified any significant risks in relation to financial sustainability during our planning.
Financial management is concerned with financial capacity, sound budgetary processes and whether the control environment and internal controls are operating effectively.	• Systems of internal control. • Budgetary control system. • Financial capacity and skills. • Arrangements for the prevention and detection of fraud.	We will review the budget and monitoring reporting by the Fund during the year to assess whether financial management and budget setting is effective. In addition, we will also ensure that there is a proper officer and fund manager who have sufficient status to be able to deliver good financial management, that monitoring reports contain information linked to performance as well as financial data, and that members have the opportunity to provide a sufficient level of challenge around variances and under-performance. Using Audit Scotland's publication "COVID-19 Emerging Fraud Risks", we will assess what action the Fund has taken to minimise risk to its control environment and internal controls. **Audit Risk:** The underlying financial performance of the Fund is not transparently reported. We have not identified any significant risks in relation to financial management during our planning. Our fraud responsibilities and representations are detailed in Appendix 1 of this report.

Wider Scope Requirements (continued)

Audit Dimensions (continued)

Audit dimension	Areas to be considered	Impact on the 2020/21 Audit
Governance and transparency is concerned with the effectiveness of scrutiny and governance arrangements, leadership and decision making, and transparent reporting of financial and performance information.	• Governance arrangements. • Scrutiny, challenge and transparency on decision making and financial and performance reports. • Quality and timeliness of financial and performance reporting.	We will review the Fund's papers and use our attendance at Pension Fund Committee meetings to assess the effectiveness and scrutiny of governance arrangements. We will also review other aspects of governance around the Fund including Codes of Conduct for officers and members and fraud and corruption arrangements for reporting regulatory breaches to the Pensions Regulator. In addition, we will review the Annual Governance Statement and Governance Compliance Statement to confirm the governance arrangements observe the guidance issued by Scottish Ministers. We will review the work undertaken in relation to risk management including updates to the policies in place as a result of COVID-19 and whether these are appropriate for the longer-term. **Audit Risk:** The Fund's approach is not keeping pace with good practice. We have not identified any significant risks in relation to governance and transparency during our planning.
Value for money is concerned with using resources effectively and continually improving services.	• Value for money in the use of resources. • Link between money spent and outputs and the outcomes delivered. • Improvement of outcomes. • Focus and pace of improvement.	We will gain an understanding of the Fund's self-evaluation arrangements to assess how it demonstrates value for money in the use of resources and the linkage between money spent and outputs and outcomes delivered. We will also review the scrutiny that is in place to challenge the Fund's investment managers on fees and performance. **Audit Risk:** The Fund does not have sufficient scrutiny over the expenditure of the Fund. We have not identified any significant risks in relation to value for money during our planning.


Maintaining
audit quality

Maintaining audit quality

Responding to challenges in the current audit market

This is a time of intense scrutiny for our profession with questions over the role of auditors, market choice and the provision of non-audit services by an audit firm. We welcome the debate and are engaging fully with all parties who have an interest in the current audit market reform initiatives, so that our profession, our people, our clients and most importantly, the public interest, are served to the highest standards of audit quality and independence.

The role of audit	• Public confidence in audit has weakened over recent years and the expectation gap has widened with differences between what an audit does and what people think it should do (largely in areas of internal controls, fraud, front half assurance and long term viability). • Deloitte fully supports an independent review into the role of auditors. • The Government's Brydon Review will consider UK audit standards and how audits should evolve.
Would it be better to have audit only firms?	• Deloitte believes that multidisciplinary firms have more knowledge, greater access to technology and a deeper talent pool. The specialist input from industry, valuation, controls, pensions, cyber, solvency, IT and tax services are critical to an effective audit. • Our investment in audit innovation, training and technology is greater because of the multidisciplinary model.
Is the current audit market uncompetitive?	• We recognise that the competition for large, complex clients is fierce, but we wholeheartedly support greater choice being available to stakeholders. • There are barriers to entry in the listed market that are significant including the required global reach, unlimited liability, and the high cost of tendering. • The audit profession has engaged with the Competition and Markets Authority with ideas on how to provide greater choice in the market, and responded to the CMA's suggested market remedies.
Independence and conflicts from other services	• Legislation and the FRC's Ethical Standard restrict the services we may provide to audit clients. • Deloitte invests heavily in systems, processes and people to check for potential conflicts. • We have governance in place to assess any areas of potential conflict, including where required to protect the public interest. • Fees for non-audit services to audit clients have fallen since 2008 (17% to 7.3% of firm revenue).
Deloitte	• Deloitte and Audit Service Line leadership are happy to meet the Board and management of our clients with respect to this important debate. We reaffirm our commitment to quality, independence and upholding the public interest • Our Impact Report and Transparency Report are available on our website https://www2.deloitte.com/uk/en/pages/about-deloitte-uk/articles/annual-reports.html • Our response to the latest AQRT report is on page 22

Our approach to quality

AQR team report and findings

Audit quality remains our number one priority and we have a relentless commitment to it. We continue to invest in and enhance our Audit Quality Monitoring and Measuring programme.

In July 2020 the Financial Reporting Council ("FRC") issued individual reports on each of the seven largest firms, including Deloitte, on Audit Quality Inspections providing a summary of the findings of its Audit Quality Review ("AQR") team for the 2019/20 cycle of reviews.

We greatly value the FRC reviews of our audit engagements and firm wide quality control systems, a key aspect of evaluating our audit quality.

We are pleased with our results for the inspections of FTSE 350 entities achieving 90% assessed as good or needing limited improvement, which included some of our highest risk audits. Our objective is for 100% of our audits to be assessed as good or needing limited improvement and we know we still have work to do in order to meet this standard. We are however, extremely disappointed one engagement received a rating of significant improvements required during the period. This is viewed very seriously within Deloitte and we have worked with the AQR to agree a comprehensive set of swift and significant firm wide actions.

We are also pleased to see the impact of our previous actions on prior year adjustments is reflected in the results of current year inspections with no findings in this areas. In addition the FRC identified good practice examples including in: risk assessment, group oversight, our comprehensive IFRS9 expected credit loss audit programme and our Pension Fund Committee reporting.

Embedding a culture of challenge in our audit practice underpins the key pillars of our audit strategy. We invest continually in our firm wide processes and controls, which we seek to develop globally, to underpin consistency in delivering high quality audits whilst ensuring engagement teams exercise professional scepticism through robust challenge.

All the AQR public reports are available on its website.

https://www.frc.org.uk/auditors/audit-quality-review/audit-firm-specific-reports

The AQR's 2019/20 Audit Quality Inspection Report on Deloitte LLP

"We reviewed 17 individual audits this year and assessed 13 (76%) as requiring no more than limited improvements. Of the ten FTSE 350 audits we reviewed this year, we assessed nine (90%) as achieving this standard."

"We have highlighted in this report aspects of firm-wide procedures which should be improved, including strengthening the monitoring of the firm's audit quality initiatives."

"Our key findings related principally to the need to:

- Improve the extent of challenge over cash flow forecasts in relation to the impairment of goodwill and other assets.
- Enhance the effectiveness of substantive analytical review and other testing for revenue.
- Improve the assessment and extent of challenge regarding management's estimates, particularly for model testing."

"The firm has taken steps to address the key findings in our 2019 public reports, with actions that included focused training and standardising the firm's audit work programs. We have identified improvements, for example in the audit of potential prior year adjustments and related disclosures, a key finding last year. We also identified good practice in a number of areas of the audits we reviewed (including effective group oversight and robust risk assessment) and in the firm-wide procedures (including the firm's milestone program, with expected dates for the phasing of the audit monitored by the firm)."

Purpose of our report and responsibility statement

Our report is designed to help you meet your governance duties

What we report

Our report is designed to establish our respective responsibilities in relation to the financial statements audit, to agree our audit plan and to take the opportunity to ask you questions at the planning stage of our audit. Our report includes:

- Our audit plan, including key audit judgements and the planned scope; and
- Key regulatory updates, relevant to you.

Other relevant communications

- Our technical updates provide the Pension Fund Committee with some insight in to relevant topical events in the pensions industry.
- We will update you if there are any significant changes to the audit plan.

This report has been prepared for the Pension Fund Committee, as a body, and we therefore accept responsibility to you alone for its contents. We accept no duty, responsibility or liability to any other parties, since this report has not been prepared, and is not intended, for any other purpose.

What we don't report

- As you will be aware, our audit is not designed to identify all matters that may be relevant to the Pension Fund Committee.
- Also, there will be further information you need to discharge your governance responsibilities, such as matters reported on by management or by other specialist advisers.
- Finally, the views on internal controls and Fund risk assessment in our final report should not be taken as comprehensive or as an opinion on effectiveness since they will be based solely on the audit procedures performed in the audit of the Annual Accounts and the other procedures performed in fulfilling our audit plan.

We welcome the opportunity to discuss our report with you and receive your feedback.

Pat Kenny

for and on behalf of Deloitte LLP

Glasgow | 26 January 2021

Topical matters

Topical matters

Cybercrime practical tips

Why protection is important

The latest Government's Cyber Security Breaches Survey for 2020 showed 46% of organisations in the UK had cyber breaches in the previous 12 months, increasing to 75% for large organisations. This is up from 24% and 65% from the Government's Cyber Security Breaches Survey conducted in 2016. COVID-19 has exacerbated this trend, with many organisations requiring people to work remotely from home which has not always allowed effective cyber security arrangements to be put in place.

The latest 2020 research also shows that the pensions sector has not evaded the impact of cybercrime. Since the introduction of the General Data Protection Regulation (GDPR), there has been 158 breaches reported to the Information Commissioners Office (ICO), 43 of which have been categorised as relating to security, unauthorised access or phishing. Some examples of successful hacking in the pensions sector include, The Japan Pensions Service, The U.S. Federal Retirement Thrift Investment Board and The Pittsburg Police Pension Fund.

The National Cyber Security Centre (NCSC) has issued some useful guidance on the steps that trustees can take to minimise the risk of falling victim to cybercrime. The key steps are detailed below:

Suggested steps	Practical application
Use a firewall to secure internet connections	Pension schemes and their third party providers should ensure that internet connections are protected with a firewall. This effectively creates a 'buffer zone' between the IT network and other external networks.
Choose the most secure settings for devices and software	Check the settings of devices and software used by the scheme to make sure they have the highest security settings as manufacturers often set the default configurations of new software and devices to be as open and multi-functional as possible.
Control who has access to scheme data and services	Staff and administrators should have just enough access to software, settings, online services and device connectivity functions in respect of the scheme to allow them to perform their role. Extra permissions should only be given to those who need them and should be monitored and controlled regularly.
Protection from viruses and other malware	Anti-virus software should be installed on all computers and laptops that are used on scheme activities. Smartphones and tablets should be configured in accordance with NCSC's guidance in which case additional antivirus software may not be necessary.
Keeping devices and software up to date	No matter which phones, tablets, laptops or computers pension schemes and their outsourced providers are using, it is important they are kept up to date at all times through the installation of regular updates that are released. This is true for both operating systems and installed apps or software.

Topical matters

Cybercrime PRAG protection guidance

In October 2020, the Pension Research Accountants Group (PRAG) issued updated guidance on cybercrime protection. These slides have been compiled using information and examples contained within the PRAG Cybercrime Protection Guidance October 2020 document.

In combatting the risk of cybercrime on the scheme, the PRAG guidance suggests that trustees should focus on the key areas detailed below.

1. Understand the scheme's vulnerability to cybercrime

It is possible to assess the extent to which a pension scheme is vulnerable to cybercrime, so that a proportionate response can be taken to this problem. The trustees should ask themselves:

a. How attractive is a pension organisation to cybercriminals?

The scheme data is likely to contain a lot of personal information such as name, address, bank account details etc that would be attractive to cybercriminals. In addition, sensitive information is likely to be held such as health and vulnerability of individual members which could be used to target individuals directly. The pension scheme data is therefore likely to be very attractive to cybercriminals making the majority of schemes vulnerable to attack.

b. What damage would be caused to a pension scheme by cyber breaches?

A successful cybercrime attack is likely to undermine the reputation of the responsible stakeholder of the scheme, be it the sponsoring employer(s), the administrator of the scheme and the trustees. The scheme will likely hold many items of sensitive data and the failure to not protect this could cause long lasting damage both financially and to the reputation of the responsible party that was the subject of the breach. Trustees should consider both the direct and consequential risks of a cybercrime attack. It may be that because of the inherent link to the sponsoring employer, a coordinated approach between the trustees and the sponsor to the controls and processes to mitigate the risk of a cybercrime attack is warranted.

PRAG recommend the following key actions:

- **Map the scheme's data to establish** – the nature of data held, where the data is held and the responsible party for that data. The mapping of data should be updated regularly.
- **Understand how data is passed between systems and users and the data security controls in place** – for most schemes the data flows between employers, administrators and other third parties such as the actuary and the auditor. Examples of security controls are password protection, secure data transfer portals, regular penetration testing and secure data back-ups and storage. Trustees should ask key suppliers for access to penetration testing results where not specifically mentioned in a third party controls report and ensure that data back-ups have occurred regularly for the scheme. A regular review programme of third party providers internal controls reports is recommended with follow up enquiries made in respect of relevant exceptions.
- **Consider crisis management planning** – it is a mistake to rely on complete security against an attack. Scenario crisis management training can be important to allow trustees to respond to the attack as it happens and establish who the key decision makers are and who can/will provide the trustees with expert technical support. Incident planning should be reviewed at least annually.
- **Establish arrangements for the Investigation of an attack** – knowing the extent of the attack, what data may have been stolen and what weakness allowed the attack to happen are vitally important steps to be able to report the cyber breach, mitigate the impact of the breach and implement revised controls to prevent a future attack.
- **Establish a communications plan** – if there is a data breach, the trustees will need to communicate with the affected members, other stakeholders , handle external press enquiries and report to the Information Commissioner's Office (ICO).

Topical matters

Cybercrime PRAG protection guidance (continued)

2. Ensure the scheme is resilient to cybercrime

The actions noted on the previous slides are considered to be pre-emptive actions that the trustees should take. This is a key part in building the schemes resilience to cybercrime. Once the pre-emptive actions have been taken, the trustees should consider addressing any identified vulnerabilities and strengthening its protection levels. Action plans should include prioritised recommendations that are allocated to a specific organisational function or individuals. There are two main areas for ensuring the scheme is resilient to cybercrime.

a. Plan for resilience

The trustees should have an established plan to ensure resilience in the face of a cyberattack. The key areas are:

- An agreed cybercrime response plan that has defined roles and responsibilities. This plan should be updated regularly to ensure all parties clearly understand their role within the plan.
- Inclusion of cyber risk and information security on the risk register along with documentation of the associated controls. The nature of the risk, the adequacy of the controls and when the controls were last tested should be included in the risk register. The identification of controls and when the controls were last tested are common omissions from the risk registers that we see as part of our audits.
- Addressing identified vulnerabilities is a key part of planning for resilience. Trustees should identify those systems and controls that should be prioritised and introduce processes to develop continuous monitoring and testing of those controls. Trustees may wish to embed cyclical testing of these processes and controls in to an internal audit plan.

b. Reactive action

A key element of ensuring the scheme is resilient to cybercrime is being able to be reactive to incidents as the occur. Trustees and their providers need to be able to act swiftly to stop the incident, contain it and recover normal operations as quickly as possible. The incident response plan noted previously should allow the trustees to take the following reactive actions:

1. **Incident triage** – swift immediate action utilising the relevant specialists to contain the incident, protect the scheme against further damage, restore normal operations and then work to eradicate the threat.
2. **Crisis communications and media management** – contacting affected members, managing key stakeholders and handling any media enquiries.
3. **Investigate** – it is important to quickly investigate and determine what happened and who is affected. Trustees will likely need support from specialists in this area to uncover the severity of any breach and understand the recovery options that are available, for example alerting affected parties quickly to prevent any further damage be it reputational or financial.
4. **Mitigate the impact** - trustees should look to minimise the legal consequences, mitigate fines and penalties that may occur and be proactive in their media releases and concentrate on restoring confidence and its reputation.

Deloitte response: The items discussed above and on the previous slides should help the trustees pre-empt a cybercrime attack, manage the attack and then mitigate the impact of the attack on the scheme and the affected people. By taking the actions noted, the trustees and the scheme should be able continue to fulfil key functions even in the face of a cyberattack. The full PRAG guidance is available on the PRAG website. The trustees may wish to obtain and review the full guidance to aid them further in their cyber crime planning.

Topical matters

Cybercrime glossary

When dealing with the complexity of cybercrime there are many complex terms that are often used but can be difficult to understand. It is important to have an understanding of the terminology and the risks faced to truly be able to plan for and mitigate against the many different types of cybercrime. The glossary below has been compiled using the PRAG Cybercrime Protection Guidance October 2020 document.

Phishing

Phishing has been undertaken for many years. It has been defined as 'the dishonest attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication'.

'Spear phishing'- directed at a specific individual rather than randomly sending out thousands of emails, and often preceded by the gathering of information about the intended recipient's interests and vulnerabilities;

'Clone phishing'- is where a previously legitimately sent email, is obtained, altered to include new illegitimate links (and sometimes infected with malware), and re-sent to the original recipient in the hope that its' familiarity will ensure that it is opened;

'Whaling'-is a form of 'spear phishing' targeted at celebrities and senior executives where there is felt to be a significant financial gain. Significant research in to the intended recipient can precede whaling;

'Link manipulation'- is where an intended victim is sent URL link which looks very much like another one which they are familiar with, but which is actually different. For example, instead of a genuine bank customer services page at say www.abcbank.com/customerservices a URL link which is www.abcbank.customerservices.com;

'Filter evasion'- is where the intended victim is sent a photo or video of a nature felt likely to induce them to look at or play it. When this happens either the victim has to provide their email and password or malware downloads;

'Website forgery'- involves websites being forged to look almost exactly like the genuine one but opening it or moving between the pages can infect the user's computer;

'Covert re-direct'- is where the website may be genuine but 'pop ups' are not and in removing them from the screen, the victim's computer can be infected;

'Phishing'- can also be **'vishing'** (voice phishing) and **'smishing'** (short message phishing). In respect of vishing, commonly available apps can be used to alter the number appearing on a smartphone as the caller to make it appear genuine and recognised, to alter the voice and to add background office or other noise.

Ransomware

Ransomware can encrypt the victim's files, making them inaccessible, and result in a demand for a ransom payment to decrypt them. The May 2017 'Wannacry' global cybercrime attack (named after the particular malware virus) encrypted up to 70,000 computers in the NHS, other networks in 150 countries and cost in the region of $4 billion.

Ransomware can also be non-encrypting. It can involve the loading of images on to computer screens or requiring the re-loading of Windows software – both to be avoided in return for the payment of a ransom. There is also **Leakware** which threatens to publish stolen information from the victim's computer system.

Mobile ransomware is used to display a blocking message over top of all other applications for Android phones and to use the Find My iPhone system to lock access to an iphone.

Topical matters

Pension scams

A major event like COVID-19 can initiate new types of scam activity. Trustees should be aware that the scam activity often appears after the initial shock of a major event such as the COVID-19 pandemic. In a recent press release by The Pensions Regulator (TPR) and the Financial Conduct Authority (FCA) it was estimated that a total of £30.9m has been reportedly lost to pension scammers since 2017 according to complaints filed with Action Fraud. Scammers targeted pension pots big and small, with reported losses ranging from under £1,000 to as much as £500,000 and the average victim being a man in his fifties.

When it comes to the pensions sector, there have been a number of high profile scams in respect of **financial advice** and **authorised transfers**. However, recently we have become aware of a number of direct attempts that have been made regarding the **disinvestment of assets and the re-direction of the sales proceeds** by scammers. In a recent event, hackers were able to gain access to the email accounts of scheme management using phishing emails and were able to prepare a disinvestment instruction to the global custodian, update the bank account details to their own personal bank account and **successfully misappropriate the cash away from the scheme**. In this particular example, there were a number of factors that lead to the scammers being able to de-fraud the pension scheme:

- The use of phishing emails;
- The disinvestment process and retention of previous instructions in email accounts; and
- Control failings at the global custodian that did not follow their own internal controls for bank account changes.

In light of the above case study example, trustees' may wish to review their internal controls around the disinvestment process to ensure they are best protecting themselves against scammers.

The above example highlights that scammers are becoming more sophisticated, opportunistic and daring, and will try to get personal details or money from victims/schemes in many ways. Scammers tend to target people who are more vulnerable or susceptible to being scammed. This has been made more likely in the current climate with many more people working at home, being isolated or outside of what may ordinarily be a secure IT environment/connection.

Trustees should therefore ensure that members are aware of the following steps communicated by the FCA to protect their members against pension scams:

1. Use the Financial Services Register and Warning List to check who you are dealing with.
2. Reject offers that come out of the blue.
3. Beware of adverts on social media channels and paid for/sponsored adverts online.
4. Do not click links or open emails from senders you do not already know.
5. Avoid being rushed or pressured into making a decision.
6. If a firm calls you unexpectedly, use the contact details on the Register to check that you are dealing with the genuine firm.
7. Do not give out personal details (bank details, address, existing insurance/pensions/investment details).

Deloitte response: With a noticeable increase in scams as a result of COVID-19, pension schemes and individual members are a likely target of scammers and cyber fraudsters as they hold large amounts of personal data and assets. It is critical for trustees and scheme managers to take steps to protect their members and assets, and be aware of the common types of scam impacting the pensions industry. This is an issue which all trustees and scheme managers, regardless of the size or structure of their scheme should be alert to.

Appendices

Key audit matters

Appendix 1: Fraud responsibilities and representations

Responsibilities explained

Your Responsibilities:

The primary responsibility for the prevention and detection of fraud rests with management and the Pension Fund Committee, including establishing and maintaining internal controls over the reliability of financial reporting, effectiveness and efficiency of operations and compliance with applicable laws and regulations.

Our responsibilities:

- We are required to obtain representations from your management regarding internal controls, assessment of risk and any known or suspected fraud or misstatement.
- As auditors, we obtain reasonable, but not absolute, assurance that the Annual Accounts as a whole are free from material misstatement, whether caused by fraud or error.
- As set out in the significant risks section of this document, we have identified management override of controls as a key audit risk for the Fund.

Fraud Characteristics:

- Misstatements in the Annual Accounts can arise from either fraud or error. The distinguishing factor between fraud and error is whether the underlying action that results in the misstatement of the Annual Accounts is intentional or unintentional.
- Two types of intentional misstatements are relevant to us as auditors – misstatements resulting from fraudulent financial reporting and misstatements resulting from misappropriation of assets.

We will request the following to be stated in the representation letter signed on behalf of the Pension Fund Committee:

- We acknowledge our responsibilities for the design, implementation and maintenance of internal control to prevent and detect fraud and error.
- We have disclosed to you the results of our assessment of the risk that the Annual Accounts may be materially misstated as a result of fraud.
- We are not aware of any fraud or suspected fraud / We have disclosed to you all information in relation to fraud or suspected fraud that we are aware of and that affects the Fund and involves:
  (i) management;
  (ii) employees who have significant roles in internal control; or
  (iii) others where the fraud could have a material effect on the Annual Accounts.
- We have disclosed to you all information in relation to allegations of fraud, or suspected fraud, affecting the Fund's Annual Accounts communicated by employees, former employees, analysts, regulators or others.

Appendix 1: Fraud responsibilities and representations (continued)

Inquiries

We will make the following inquiries regarding fraud:

Management:

- Management's assessment of the risk that the Annual Accounts may be materially misstated due to fraud, including the nature, extent and frequency of such assessments.
- Management's process for identifying and responding to the risks of fraud in the Fund.
- Management's communication, if any, to the Pension Fund Committee regarding its processes for identifying and responding to the risks of fraud in the Fund.
- Management's communication, if any, to employees regarding its views on business practices and ethical behaviour.
- Whether management has knowledge of any actual, suspected or alleged fraud affecting the Fund.
- We plan to involve management from outside the finance function in our inquiries.

Internal audit

- Whether internal audit has knowledge of any actual, suspected or alleged fraud affecting the Fund, and to obtain its views about the risks of fraud.

The Pension Fund Committee

- How the Pension Fund Committee exercises oversight of management's processes for identifying and responding to the risks of fraud in the Fund and the internal control that management has established to mitigate these risks.
- Whether the Pension Fund Committee has knowledge of any actual, suspected or alleged fraud affecting the Fund.
- The views of the Pension Fund Committee on the most significant fraud risk factors affecting the Fund.

Appendix 2: Independence and fees

A Fair and Transparent Fee

As part of our obligations under International Standards on Auditing (UK), we are required to report to you on the matters listed below:

Independence confirmation	We confirm the audit engagement team, and others in the firm as appropriate, Deloitte LLP and, where applicable, all Deloitte network firms are independent of the Fund and will reconfirm our independence and objectivity to the Pension Fund Committee for the year ending 31 March 2021 in our final report to the Pension Fund Committee.
Fees	Our fees for the audit for the year ending 31 March 2021 will be communicated to you separately. There are no non-audit services fees proposed for the period.
Non audit services	In our opinion there are no inconsistencies between the FRC's Ethical Standard and the Fund's policy for the supply of non-audit services or any apparent breach of that policy. We continue to review our independence and ensure that appropriate safeguards are in place including, but not limited to, the rotation of senior partners and professional staff and the involvement of additional partners and professional staff to carry out reviews of the work performed and to otherwise advise as necessary.
Relationships	We have no other relationships with the Fund, the Pension Fund Committee, or management, and have not supplied any services to other known connected parties.

Deloitte.