DF/23/72
Devon Pension Board
6th July 2023

# ACTIONS AND RECOMMENDATIONS TRACKERS

Report of the Director of Finance and Public Value

Please note that the following recommendations are subject to consideration and determination by the Committee before taking effect.

## 1) Recommendation

That the Board be asked to:

(a) Note the progress made on completing actions arising from internal audits and pension board recommendations and requests

## 2) Introduction

2.1 As part of an agreed actions from previous board meetings an Audit action log has been created to track progress and completion of audit actions and recommendations. In addition, officers have also produced a log of actions and requests raised by the Pension

## 3) Trackers

3.1 The Actions and Recommendations tracker (Appendix 1) compiles a list of actions, recommendations and requests raised by the Devon Pension Board. Previously completed actions have been removed.

3.2 Final audit reports issued relating to 2022/23 audits that have not already been brought to the board are as follows

- Cyber Security
- Escrow Account

The above reports are attached to this report.

## 4) Cyber Security

4.1 The Cyber Security audit was undertaken in 2022/23 for both the pension fund and Peninsula Pensions. The overall rating applied to this audit was that of Limited Assurance, indicating that there were several gaps and areas of weakness to be addressed.

4.2 Officers have been working on their respective actions and as requested by the board at the last meeting, the table below summaries the progress to date. Audit are due to undertake a follow up audit later in the year.

| **Section 1 – Risk not identified to mitigate against threats** | | | | | |
|---|---|---|---|---|---|
| High | High (remaining) | Medium | Medium (remaining) | Low | Low (remaining) |
| 2 | 0 | 2 | 1 | 2 | 0 |
| **Section 2 – Suppliers or partners disclose or disrupt the service (supply chain management)** | | | | | |
| High | High (remaining) | Medium | Medium (remaining) | Low | Low (remaining) |
| 2 | 2 | 4 | 1 | 0 | 0 |
| **Section 3 – Unauthorised modification or deletion of data** | | | | | |
| High | High (remaining) | Medium | Medium (remaining) | Low | Low (remaining) |
| 1 | 0 | 3 | 0 | 0 | 0 |
| **Section 4 – Poor user understanding of cyber risks** | | | | | |
| High | High (remaining) | Medium | Medium (remaining) | Low | Low (remaining) |
| 2 | 0 | 1 | 0 | 0 | 0 |
| **Section 5 – Recovery process fail following a cyber attack or IT disruption** | | | | | |
| High | High (remaining) | Medium | Medium (remaining) | Low | Low (remaining) |
| 3 | 3 | 1 | 0 | 1 | 1 |

4.3 Both of the fund's main suppliers, namely Brunel and Heywood have undertaken cyber security reviews or audits during the year. Brunel received a positive audit from Deloitte whilst Heywood have undertaken a review. The Heywood review is attached to this report for the board's information.

## 5) Conclusion

5.1 The Board is asked to note the progress on completing requests made by the pension board and work undertaken to date on audit actions.

**Angie Sinclair**
Director of Finance and Public Value

**Electoral Divisions**: All

## Local Government Act 1972: List of background papers

Nil

**Contact for enquiries:**
Name: Charlotte Thompson
Telephone: 01392 381933
Address: Room 180 County Hall

Appendix 1

**DEVON PENSION BOARD**
**ACTIONS AND RECOMMENATIONS TRACKER**

The actions tracker allows Board members to monitor responses, actions and outcomes against their recommendations or requests. The tracker will be updated following each board. Once an action has been completed, it will be shaded out to indicate that it will be removed from the tracker at the next meeting.

| Date | Recommndations / Actions | Response | Progress |
|---|---|---|---|
| 04/05/2022 | 46 - further info/signposting to climate change policy in risk register | | New control added that refers to the Investment Strategy Statement and adopting Brunel's climate policy |
| 18/10/2022 | 76 - PP reporting, consideration to include historic 12 months figures | | included in performance report July 2023 |
| 18/10/2022 | 79 - breaches as a standing item even if there are none to report | | Added to contribution monitoring report July 2023 |
| 07/02/2023 | 92 - include connecting to the Pensions Dashboard in the risk register | | completed July 2023 |
| 18/04/2023 | 100 - provide update on the progress of actions from the cyber security audit | | included in the audit and actions report July 2023 |
| 18/04/2023 | 104 - update Pension Board annual report with Colin Shipp's leaving date | | completed |

# Internal Audit Report - Final

# Devon Pension Fund - Cyber Security 2022-23

## Devon County Council / Devon Pension Fund

February 2023

devon audit partnership
Auditing for Achievement

## Service Objective

To ensure the Confidentiality, Integrity, and Availability of Devon Pensions Funds data and subsequent systems.

## Audit Opinion

**Limited Assurance** -Significant gaps, weaknesses or non-compliance were identified. Improvement is required to the system of governance, risk management and control to effectively manage risks to the achievement of objectives in the area audited.

| Assurance Opinion on Risks or Areas Covered<br>- *key concerns or unmitigated risks* | Level of Assurance |
|---|---|
| **Risks are not identified to mitigate against threats to the IT infrastructure (Risk Management).**<br>- *There are no cybersecurity risks recorded on the DPF risk register (although there are on Peninsula Pensions risk register).*<br>*Some of the mitigating controls for some risks may not be appropriate or have been omitted.* | **Limited Assurance** |
| **Suppliers or partners disclose information or disrupt the pension service (Supply Chain Management).**<br>- *Lack of minimum requirements (standard operating procedures) in place regarding the management of suppliers.*<br>- *Lack of detail regarding the roles and responsibilities of both parties in the event of a cyber-attack for Altair or Logotech.* | **Limited Assurance** |
| **Unauthorised modification or deletion of data (Access controls).**<br>- *The current link to access Logotech uses Internet Explorer which stopped receiving support/security updates from June 25, 2022.*<br>- *No standardised documented procedure for the creation/removal of user access. (Altair & Logotech).* | **Reasonable assurance** |
| **Poor user understanding of cyber-risk and security procedures results in the disclosure of information (Training).**<br>- *Mandatory training not being completed by all staff or Board/Committee Members.* | **Limited Assurance** |
| **Devon County Council (DCC) recovery processes fail following a cyber-attack or IT disruption (DPF and PP BC & DR plans).**<br>- *There is no scheduled testing for DPF/Investments Team nor PP's BCP, and there has not been a test completed within the past 12 months.*<br>- *A number of further areas where improvements can be made.* | **Limited Assurance** |

## Introduction

The Local Government Pension Scheme is a valuable renumeration package for employees working for organisations that are participating in the pension scheme. The Devon Local Government Pension Scheme (LGPS) is managed by Devon County Council (DCC) via the Devon Pension Fund (DPF), who act as the administering authority. Peninsula Pensions (PP) was formed in September 2013 following the merger of the pension administration services of DCC and Somerset County Council. PP manages all aspects of pension fund administration, including maintaining member records, calculating and paying employee benefits. Our audit focused on the two operational teams supporting the DPF; the DCC Investments Team and PP.

The Institute for Internal Auditor's 2023 Risk in Focus has Cyber security and data security as the top risk an organisation will face within the next three years. Due to recent geo-political issues, the threat landscape has become ever more dangerous, with ransomware attacks increasing by 80% in 2022. Organisations are improving their cyber defences which has led to attackers shifting their focus towards third-party suppliers as a means of gaining access to an organisation's IT infrastructure.

Pension schemes hold large amounts of personal data and assets which can make them a target for threat actors. Consequently, the Pensions Regulator requires workplace pension trustees and scheme managers to protect pension scheme members and assets from cyber security threats. The Pensions Regulator has published cyber security principles to help pension schemes manage their cyber risks.

The pension fund is reliant on the DCC IT network and infrastructure for its operational activity and also on specific cloud-based applications. A robust control framework is needed to ensure that the pension fund is aware of cyber risk and controls required to mitigate the risks, alongside holding the responsibility to ensure that Business Continuity Plans and Disaster Recovery Plans (BCP/DR) are suitable and up to date.

The Objective of the audit was to evaluate Devon Pension Fund's control framework in relation to Cyber Security, using the Pensions Regulator's (TPR's) cyber security principles as a standard, to provide assurance that cyber risks are being effectively managed. TPR′s cyber security principles, include Risk Management, Supply Chain Management, Access Controls, Staff Awareness and BCP/DR. The risks above encompass a significant proportion of the Pensions Regulator's cyber security principles.

A Cyber Security audit relating to the core DCC control framework, focussing on the control areas covered by Cyber Essentials as well as core back up arrangements and Business Continuity, was completed in March 2021 and followed up in March 2022, including additional testing, and also followed up in September 2022. The overall audit opinion, regarding the effectiveness of the risk areas was "Limited Assurance". This was in large part due to the current weaknesses with the Corporate ICT Business Continuity Plans, including Disaster Recovery. However, there is an active ICT project regarding improving those plans. Adequate controls were found to be in place regarding; Corporate Firewall, Access controls, Secure Configuration, Malware protection and Security Updates/Patch Management.

An audit regarding DCC Cyber Governance was completed in September 2022. Limited assurance was provided regarding the governance arrangements concerning Cyber Security threats/risks.

Pensioners' data is stored via "Altair", the pensions administration system, which is provided by Heywood's and is externally hosted (outside of the DCC infrastructure). Investment data is stored via "Logotech", the pension funds investment record system, which is also externally hosted.

The Devon Pension Fund is a member of the Brunel Pension Partnership (BPP). The BPP is one of eight UK Local Government Pension Scheme pools, bringing together £35 billion of investments of ten funds: Avon, Buckinghamshire, Cornwall, Devon, Dorset, the Environment Agency, Gloucestershire, Oxfordshire, Somerset and Wiltshire. Brunel is authorised and regulated by the Financial Conduct Authority as a full-service Markets in Financial Instruments Directive (MiFID) firm. It is understood that the BPP also hold DPF investment data.

## Executive Summary

We have identified a number of areas where we consider there to be significant gaps in the control framework.

The overall cyber security risk is recognised on the Devon County Council's (DCC) corporate risk register, and it is also recorded within the Peninsula Pension's (PP) risk register. However, cyber security risks are not recorded within the DPF risk register which weakens governance and decision making regarding the risks identified and their potential mitigations.

The risk owners in place are experienced, but they have not received specific training in relation to cyber security nor risk management, yet there is evidence of the use of reputable external resources to support the mitigation and control of risks. Risk registers are a standing item on the agendas of the DPF Board meetings to discuss and scrutinise risks, including cyber security risks.

While the Peninsula Pensions risk register included the risk of supplier failure, it did not include a mitigating control for the management of suppliers. The DPF risk register does not currently include any risks in relation to the failure of suppliers.

Regarding Heywood's (Altair), there is adequate supplier management in place. Annual meetings take place to discuss security requirements and emerging risks. Heywood's supply communication on current topical areas of concern (the war in Ukraine for example), alongside having security review reports and accreditations, are available upon request.

Regarding Logotech, supplier management is limited. Ongoing assurance is not routinely obtained to confirm that their cyber security risks are being managed effectively, and there are currently no established processes in place to determine the cyber security posture of Logotech. These weaknesses are detailed in our observations below.

There is a contract in place, as well as supporting license terms and conditions, which state the responsibilities of both Heywood's and Peninsula Pensions (DCC) for the use and maintenance of the system. However, the contract does not state the roles and responsibilities of both parties in the event of an incident. We were not able to obtain a copy of a contract with Logotech.

As part of this audit, we arranged for a cyber security questionnaire to be sent to each of the suppliers/partners. We identified no significant immediate concerns regarding the responses received from Heywood's regarding Altair. At the time of reporting there had been no response from Logotech or Brunel. The responses are included in Appendix D. We have made observations to obtain further information/assurance from the suppliers.

Neither DPF nor PP maintain an Information Asset Register. This is an expectation of the ICO to meet UK data protection legislation requirements and it can assist in the understanding and management of supplier risk.

Mandatory cyber security training is available to all DCC staff and Members, however, not all PP, Investments Team staff or DCC Members on the Pension Board have completed the training or signed the relevant policy. The table below shows the percentage of those that have not completed the mandatory requirements.

| DPF Operational Teams (No. of Staff) | Cyber Security Awareness Training | Personal Information Security Policy |
|---|---|---|
| DCC Investments Team (6) | 33% | 17% |
| Peninsula Pensions (72) | 17% | 29% |
| Members (8) | 75% | 88% |

There are Business Continuity Plans (BCP) for Devon Pension Fund (DPF) and Peninsula Pensions (PP), which use approved templates from Devon Emergency Planning Service. Both outline a cyber-attack/IT disruption as a reason to invoke the plan. The template requires confirmation of critical systems that need to be restored, alongside the priority of restore and "Recovery Time Objective" in the event of an incident. However, we have identified a number of areas for

improvement regarding the content and management of the BCP plans in our observations below including conducting a specific Cyber BC exercise.

Although reasonable, Altair and Logotech system access controls should be further strengthened by management controls to provide greater assurance in this area and our observations have been detailed below. Our observations focus on the management controls in place, and there were no concerns found with the services that Heywoods / Altair provide.

It is noted from the DCC Main Accounting System audit from October 2022, there were weaknesses identified in the administration of the user accounts for the online banking system. However, there are compensating controls in place with further actions being undertaken by the responsible officer to improve the controls in this area.

Positively, in line with external guidance from Pensions and Lifetime Savings Association, PP have recently developed a Cyber Security Policy, which references the DCC framework of IT security policies and procedures that are in place.

The detailed findings and our observations regarding these issues and less important matters are described in Appendix A. Our observations have been categorised to aid prioritisation. Definitions of the priority categories and the assurance opinion ratings are also given in the Appendices to this report.

## Issues for the Annual Governance Statement

The evidence obtained in internal audit reviews can identify issues in respect of risk management, systems and controls that may be relevant to the Annual Governance Statement. No issues were identified for the Annual Governance Statement.

## Acknowledgements

We would like to express our thanks and appreciation to all those who provided support and assistance during the course of this audit.

**Tony Rose**
**Head of Partnership**

## Detailed Audit Observations and Action Plan

| 1. Risk Area: Risks are not identified to mitigate against threats to the IT infrastructure (Risk Management). | Level of Assurance |
|---|---|
| | Limited Assurance |

**Opinion Statement:**

Our review of both Devon Pension Fund (DPF) and Peninsula Pensions (PP) Risk Registers identified that cyber security risks were not recorded on DPF's Risk Register, but they were recorded on PP's Risk Register. Both sets of Risk Registers have been reviewed in the previous six months. The lack of cyber risks on DPF's Risk Register was previously identified in our Risk Management audit (August 2022). Despite Logotech being a relatively low-risk system, as it does not hold personal data, it is used for DPF/Investment Team operations and there is a need for DPF to recognise cyber risks in its risk register.

The risk owners for DPF/PP both have experience in reviewing risks, although they have not received any risk management training in their current roles. Furthermore, neither has received any specific training in relation to cyber security risks. However, both risk owners demonstrated the use of reputable external sources to gain knowledge in the subject area.

The Devon Pension Board has a standing item in their agenda to discuss and, as part of their role, review the risk registers at each meeting. The Investment and Pension Fund Committee review the Devon Pension Board Minutes providing additional oversight.

As referred to in risk four, there is a low completion rate of mandatory cyber security and data protection training for DCC members, and no established cyber security training for non-DCC members.

We have made a number of observations below where improvements should be made.

| No. | Observation and Implications | Impact / Priority | Management response and action plan including responsible officer | |
|---|---|---|---|---|
| 1.1 | **DPF -** There are no cybersecurity risks on the DPF risk register, including the potential loss of availability of a critical externally hosted system or a partner's system(s).<br>Without cyber risks being included in the risk register, then cyber risks will not be reported, considered and then appropriate mitigating controls put in place and reviewed.<br>It is acknowledged that the risk of cyber-attack is identified on the DCC corporate risk register, as an overarching risk across the Council. This means that the risk would appear on the DPF risk register if displayed via the available dashboard. However, it is not the dashboard that gets reported to the Board. Furthermore, the corporate risk register does not include specific mitigating controls for DPF specific risks. | High | **Agreed**, risk register will be amended. | |
| | | | Responsible Officer: Charlotte Thompson | Target Date:31.01.23 |

| | | | |
|---|---|---|---|
| 1.2 | **PP** - Some of the mitigating controls for some risks may not be appropriate or omitted. For example:<br>- PP10 data & system security - mitigating control 2 – *"The system is subject to regular checks by internal audit"*.; Internal Audit is a third level control. Not considered a primary mitigating control. Other more robust controls should be identified first.<br>- PP10 data & system security - mitigating control 3 - There is only mention of GDPR training, and none of the cyber security training which is also relevant. It should be noted that cyber security training is mandatory, however, our testing found that not all staff have completed this training.<br>-PP17 - Supplier Management is not identified as a mitigating control.<br>- PP18 - mitigating control 3 – *"Information from The Pensions Regulator: You can assess how secure your scheme is and find out more about protecting yourself on the government's Cyber Essentials website. And for more information about protecting against cyber threats, visit the National Cyber Security Centre's website"*. This is not considered a mitigating control, rather just a statement of fact.<br>Documentation such as the NCSC 10 steps to cyber security and Cyber Assessment Framework may help further identify risks and additional mitigating controls.<br>DAP Risk Management Team are also available to assist with further developing the risk registers. | High | **Agreed** - The risk register can be updated to reflect this accordingly (PP10, PP17, PP18).<br>Responsible Officer: Rachel Lamb / Alexander Thompson<br>Target Date: 31/03/2023 |
| 1.3 | **PP** - The current risk score for item PP18 is a Medium (10), however, the main cyber risk on the corporate risk register for a successful cyber-attack (BI21), has a risk score of Very High (24).<br>The disparity between scores, even when taking both sets of mitigating controls in place, suggests that the risk score for PP18 is understated. | Medium | **Agreed** – to be reviewed and amended accordingly.<br>Responsible Officer: Rachel Lamb / Alexander Thompson<br>Target Date: 31/03/2023 |

| | | | | |
|---|---|---|---|---|
| 1.4 | **PP** - The Peninsula Pensions cyber risks have not been assessed in liaison with DCC ICT or any other Subject Matter Experts (SME).<br><br>The cyber risks have been considered and compiled in isolation, with limited consultation with Subject Matter Experts (SME) or certain key officers. However, it is noted that the DCC cyber pages were used as a resource when the cyber risks were assessed.<br><br>This could mean that risks and their associated mitigating controls may not be fully understood and explored resulting in appropriate mitigating controls not being put in place. | Medium | **Agreed** – consideration to be given arranging regular meetings with SMEs to discuss cyber risks and the appropriate mitigating controls, and arranging penetration testing independent from Heywood.<br><br>As part of Devon County Council, Peninsula Pensions follow Devon County Council's existing policies on Cyber Security. Altair is remotely hosted and has been assessed separately in the report and scores well in terms of risk mitigation. | |
| | | | Responsible Officer: Rachel Lamb / Alexander Thompson | Target Date: 31/05/2023 |
| 1.5 | The Risk Owners for DPF/PP have both completed their mandatory training for cybersecurity, but they have not received any elevated training in relation to risk management or cyber security risk. It is noted that Peninsula Pension's Officers draw on external sources for information (Pensions and Lifetime Savings Associate & Pensions Administration Standards Association) when reviewing the risks.<br><br>Without appropriate cyber and risk management training, there is the potential for risks to be omitted from the registers, alongside mitigating controls. | Low | **Agreed** – PP will actively seek opportunities for elevated training in future. | |
| | | | Responsible Officer: Rachel Lamb / Alexander Thompson | Target Date: 30/06/2023 |
| 1.6 | Pension Board minutes from July 2022 show an agreed discussion point in relation to PP17 - Pensions system failure for a follow-up in the next board meeting. However, there is no record in the October 2022 minutes of this being actioned.<br><br>If action points in relation to cyber security risks are not addressed, this could lead to cyber security risks not being appropriately mitigated.<br><br>Other action points had been addressed. | Low | Reported back to the October board meeting. Note included under the risk register minutes. | |
| | | | Responsible Officer: Rachel Lamb | Target Date: Complete |

| 2. Risk Area: Suppliers or partners disclose information or disrupt the pension service (Supply Chain Management). | Level of Assurance |
|---|---|
| | Limited Assurance |

**Opinion Statement:**

The risk of supplier failure is included in the PP risk register (PP17). However, a similar risk is not identified on the DPF risk register. Despite the risk PP17 being identified on the risk register there are no mitigating controls regarding supply chain management.

Minimum security requirements are communicated to suppliers via an Information Security Questionnaire (ISQ) as part of the procurement process. This process is embedded into the DCC procurement process. ISQ's were obtained at the procurement stage for both Altair and Logotech. These ISQ's were reviewed by the Data Protection Officer and relevant SME (e.g., Technical Architects) as per standard DCC process.

There is a contract in place, and supporting license terms and conditions, which state the responsibilities of both Heywood's and Peninsula Pensions (DCC) in relation to the use of and maintenance of the system. However, we were not able to obtain a copy of a contract with Logotech. We have made an observation below regarding the importance of a contract with suppliers and the need for these to include roles and responsibilities of each party.

Regarding Heywood's, there is adequate supplier management in place. Annual meetings are conducted which are used to discuss security requirements and emerging risks from both Peninsula Pensions and Heywood's. Further meetings are held between Heywood's and Senior Operational Officers in relation to upgrades to the system. Heywood's provide Peninsula Pensions with communications on current topical areas of concern (the war in Ukraine for example), alongside having security review reports available upon request. During the audit, Heywood's informed Peninsula Pensions of a Risk Ledger which is available to customers, providing access to their security information.

Regarding Logotech, Supplier management is limited in relation to cyber security as demonstrated in the table below (also see observations, item 2.2). Ongoing assurance is not routinely obtained to confirm that their cyber security risks are being managed effectively. There are currently no established processes to determine the cyber security posture of Logotech. These weaknesses are detailed in our observations below.

As part of the review, it was established that the suppliers and partners had the accreditations and key mitigating controls detailed below:

| Supplier | DCC Procurement ISQ completed | Audit security questionnaire completed | ISO 27001 (*by UKAS certified body*) | Cyber Essentials | SOC2 Compliant | Business Continuity Plan / Disaster Recovery | Incident response plans |
|---|---|---|---|---|---|---|---|
| Heywood's | Y** | Y | Y | Y | N/A | Y | Y** |
| Bluechip / Service Express (Managed Service Provider to Heywood's) | N/A | N/A | Y | N/A | Y | Y | N/A |
| Logotech | Y | Not received back | Not known | Not known | N/A | Not known | Not known |
| UKFast / ANS (Managed Service Provider to Logotech) | N/A | N/A | Not known | Y | N/A | N/A | N/A |
| Brunel Partnership | N/A | Not received back | N | Y | N/A | N/A | N/A |

** Verbal assurance acquired from the DCC Cyber Security Manager and the Information Governance Manager.

As part of the audit, we arranged for a cyber security questionnaire to be sent to each of the suppliers/partners. There were no significant concerns identified regarding the responses from Heywood's for the Altair system. Although we have made observations under this risk regarding obtaining further information regarding backups and insurance. At the time of reporting there had been no response from Logotech or Brunel. The responses are included in Appendix D.

Currently Devon Pension Fund, including the Investments Team and Peninsula Pensions, do not have an Information Asset Register (IAR). Both risk registers and the IAR assist in the understanding and management of supply chain risks.

| No. | Observation and Implications | Impact / Priority | Management response and action plan including responsible officer |
|---|---|---|---|
| 2.1 | Neither the contracts nor terms and conditions for Altair or Logotech (no contract available), specifically detail the roles and responsibilities of both parties in the event of a cyber-attack.<br><br>It is acknowledged that the roles and responsibilities are detailed for Altair in the Business Continuity Incident Management Plan. However, reference is not made to this within the contract.<br><br>A lack of a contractually agreed Incident Response Plan, detailing roles and responsibilities, increases the risk of a Cyber Incident not being managed effectively.<br><br>Contracts with suppliers/cloud providers are vital to ensure that mutual rights and obligations are stated and agreed between parties. | High | DPF – **Agreed.** Will obtain copy of contract from Logotech and progress this issue.<br><br>Responsible Officer: Charlotte Thompson — Target Date: 31.03.23<br><br>PP – **Agreed.**<br><br>Responsible Officer: Alexander Thompson / Rachel Lamb — Target Date: 01/05/2023 |
| 2.2 | There are no minimum requirements or standard operating procedures (SOPs) in place regarding the information required/ process to take for the management of suppliers and, in particular, gaining ongoing assurance for the management of cyber security risks and expected minimum controls.<br><br>For example,<br>• The Investments Team are not gaining assurance from their suppliers that their cyber security risks are being managed.<br><br>The lack of (standard operating procedures) for the management of suppliers increases the risk of inadequate assurance being obtained, leading to potentially insufficient supplier technical controls being in place to provide the level of security required. | High | DPF – **Agreed.** Will look to issue a security questionnaire on an annual basis to Logotech and Brunel.<br><br>Responsible Officer: Charlotte Thompson — Target Date:31.03.22 |

| | | | |
|---|---|---|---|
| | In an ever-changing cyber threat environment, there is also the need to continually review and communicate minimum security requirements.<br><br>Compliance with newly established minimum requirements or SOPs would help ensure such assurance is obtained.<br><br>The use of a cyber security questionnaire, seeking current detail and evidence on a periodic basis could assist in this regard. Sufficiently robust supplier management processes should be applied to all third-party suppliers. | | PP – **Agreed.** We will arrange an annual questionnaire for Heywood as with Logotech above.<br><br>Responsible Officer: Alexander Thompson / Rachel Lamb — Target Date: 01/05/2023 |
| 2.3 | There is no risk on the DPF risk register to highlight supplier risk failure. There is a risk of "Pensions System Failure" (PP17) on the PP risk register. However, there are no mitigating controls included, against PP17 regarding how assurance is gained that appropriate mitigations are obtained from suppliers in relation to cyber risk.<br><br>It would be beneficial to include a risk regarding supplier failure to ensure that all associated supplier risks & potential controls are considered, e.g. a Standard Operating Procedure and/or minimum requirements to obtain assurance e.g. from regular meetings etc. | Medium | DPF - **Agreed.** DPF risk register to be updated as suggested to cover Logotech and Brunel.<br><br>Responsible Officer: Charlotte Thompson — Target Date:31.03.23<br><br>PP - **Agreed** - The Risk Register re PP17 can be updated and made clearer accordingly.<br><br>Responsible Officer: Alexander Thompson / Rachel Lamb — Target Date: 01/05/2023 |

<table>
<tr><td>2.4</td><td>At present Devon Pension Fund, including the Investments Team and Peninsula Pensions, do not have an Information Asset Register (IAR). Data Protection legislation requires the organisation to understand and document the data that it holds, and the Information Commissioners Office (ICO) expects that this requirement is met by way of an Information Asset Register.<br><br>The ICO's website defines what an Information Asset Register is, and what it should contain, including:<br>•asset owners;<br>•asset location;<br>•retention periods; and<br>•security measures deployed.<br><br>Advice regarding the requirements of an IAR can be obtained from the DCC Strategic Information Governance Manager.</td><td rowspan="4">Medium</td><td colspan="2">DPF – Agreed. Will look into this and will produce a register if considered appropriate for DPF.</td></tr>
<tr><td>Responsible Officer: Charlotte Thompson</td><td>Target Date: 31.03.23</td></tr>
<tr><td colspan="2">PP – Agreed. Peninsula Pensions do not hold an IAR, however, we do hold information relating to data processing activities (GDPR article 30), data maps, and GDPR risk register, which demonstrate our understanding of what personal data we process, including how and why we do so, to enable us to sustain our compliance in these areas. Head of Peninsula Pensions will review the information held to ensure it complies with ICO requirement for an IAR.</td></tr>
<tr><td>Responsible Officer: Alexander Thompson / Rachel Lamb</td><td>Target Date: 01/05/2023</td></tr>
<tr><td>2.5</td><td>DCC does not have cyber security Insurance. It is unlikely that DCC would ever obtain Authority Wide Cyber Insurance. Neither does Devon Pension Fund have cyber security insurance.<br><br>During the audit, Officers have confirmed that they were not aware if the suppliers (Heywood’s and Logotech) or Partners (Brunel Partnership) have Cyber Insurance in place. We have as part of our audit work asked the relevant officers to contact the suppliers. Heywood’s have stated that they have Cyber Insurance, but no details have been provided.<br><br>It is noted that since the draft report being issued, Officers in PP have obtained evidence of cyber insurance from their supplier.<br><br>With the high risk of there being a cyber-attack, Officers and the Pensions Board should investigate, in conjunction with the DCC Strategic Cyber Security Manager, the DCC Insurance Manager and the relevant suppliers and partners, whether there is</td><td rowspan="3">Medium</td><td colspan="2">DPF – Agreed. Will enquire if Brunel/Statestreet hold such insurance.<br><br>Considering the data held on Logotech, obtaining an insurance policy would be excessive and not necessary.</td></tr>
<tr><td>Responsible Officer: Charlotte Thompson</td><td>Target Date:31.03.23</td></tr>
<tr><td colspan="2">PP – Agreed. Confirmation obtained from Heywoods of cyber insurance.</td></tr>
</table>

| | | | | |
|---|---|---|---|---|
| | necessity and affordable benefits to be had from obtaining further Cyber Insurance. | | Responsible Officer: Alexander Thompson / Rachel Lamb | Target Date: Complete |
| 2.6 | **DPF** – The Investments Team are unaware of the support available to them from Logotech in the event of a security incident.<br>Even though Logotech is a relatively low-risk system as it does not hold personal data, by establishing the support available from the supplier can help a quicker recovery of data in the event of a security incident. | Medium | **Agreed.** Will contact Logotech to establish procedures in the event of a cyber-attack. Could continue business as usual for a reasonable period without Logotech. | |
| | | | Responsible Officer: Charlotte Thompson | Target Date:31.03.23 |
| 2.7 | There is nothing in the contract with Heywood's for the continuous improvement of security within the supply chain. We have not been able to identify a contract with Logotech or an agreement with Brunel.<br>There is an opportunity to incorporate a requirement of continuous improvement of security within the supply chain within future contracts. This would provide additional assurance, through contractual obligation, that cyber security risks will be minimised. | Opportunity | DPF – **Agreed.** This will be consider in the future. As part owner of Brunel, there is a shareholder agreement in place with Brunel. | |
| | | | Responsible Officer: Charlotte. Thompson | Target Date:31.03.23 |
| | | | PP - **Agreed.** Heywood's are continuously improving security and undertake regular penetration testing. This is partly demonstrated by the move to Blue Chip in the first instance, given its SOC2 credentials. | |
| | | | Responsible Officer: Alexander Thompson / Rachel Lamb | Target Date: Complete |

| **3. Risk Area: Unauthorised modification or deletion of data (Altair & Logotech access controls).** | **Level of Assurance** |
|---|---|
| | **Reasonable Assurance** |

**Opinion Statement:**

**Altair:**

Access to Altair is suitably controlled. Although this process is not formally documented, it was established that there is adequate provisioning of accounts, alongside suitable approval mechanisms in place prior to the creation of a new user account.

Altair uses role-based access controls to manage user permissions for the system. From our review of all user accounts, we found that there were 21 user accounts who had the 'Manager Role'. The 'Manager Role' has elevated privileges which allows the most functionality, alongside the creation and deletion of users, and the amendment of the password expiry settings. Current guidance recommends applying the principle of least privilege, which means that a user account should be given only those privileges needed for them to complete their tasks.

Internal Audit was informed that a lack of MFA for Altair is due to an internal IT infrastructure restriction. Although Multi-Factor Authentication (MFA) is not place, it is acknowledged that Altair is accessed using the DCC IT environment which includes a DCC device, a VPN and unique DCC IP address. Further, each user is required to authenticate using unique credentials before authorisation is given to the user for Ping and Altair.

There are further technical controls in place to secure access to user accounts. Examples of the technical controls are:

- Unique credentials are required
- Password complexity rules are in place (12 characters, upper, lower and special characters)
- There is account lockout after three unsuccessful attempts to log in (Altair)
- Passwords are required to be changed every 30 days (Ping) / 6 months (Altair)
- Password history is enabled for the last 3 (Altair) / 12 (Ping) passwords - Meaning passwords cannot be re-used

There is an internal process in place to ensure that user accounts are removed when they are no longer required, although this process is not documented in the event of another user having to complete this task. Further to this, there are reports generated quarterly which are used to review the user accounts, including those with special access privileges. This quarterly report includes details about each user account's role(s), and these are saved within the DCC network.

Third party accounts follow the same authorisation and creation process as any other user, although it is a rare circumstance that they are needed. There are shared accounts used to access Altair which have a forced password change prior to being given to the third party requesting them. However, there is no process in place to ensure that the passwords of these accounts are changed after the prescribed period of time from when access to the shared account is given.

Authentication and authorisation logs are available in the form of reports, which are run manually. These reports are run on an ad-hoc basis, but also annually as part of the Global Journal Report. Furthermore, the aforementioned quarterly report is used as part of a house keeping process to review user accounts which have access to the system for appropriability.

Access to the Members Self Service (MSS) website for Peninsula Pension staff and users is suitably controlled. Users require unique credentials (Passwords must be at minimum 8 characters in length, including one numeric, lower case, upper case, and special character), alongside security questions, to access the MSS website. The MSS website uses HTTPS for access and had a valid digital certificate which was issued by a trusted Authority. Staff access to MSS is controlled via Altair, alongside requiring an account to access Ping.

**Logotech:**

Logotech is deemed as relatively 'low-risk' as it does not communicate with any other system or hold personal data. For example, payments cannot be placed on Logotech, it is simply a database used by the Treasury Management team for monitoring and reporting purposes.

From reviewing the list of Logotech users, we can confirm that the majority of users were appropriate, alongside their access levels. There is one example of a user on the Logotech system who no longer works within the Investment team but was subsequently removed during the Treasury Management audit.

As Logotech is used by a small Investments Team, team members are given special privileges as needed; once given, the user account loses operational abilities immediately. Multi-Factor Authentication is not used, but all users need a DCC device to connect to the DCC network as well as needing unique credentials (Username and password), which are not held to complexity rules or are required to be changed periodically.

**Online banking:**

Access to the online banking facilities is managed by DCC Finance. Access to the facility is reviewed as part of the Main Accounting System audit annually. The MAS audit October 2022 identified weakness in the administration of the user accounts with recent leaver user accounts not being removed and a lack of control over the issue of authentication cards and card readers. However, there are other compensating controls in place and actions are being taken by the Responsible Officer to ensure more robust processes are in place. This issue will be reported via the MAS audit, and it is an example of where DPF could enhance its risk awareness by liaising with Finance regularly to obtain assurance over the status of systems that they use. We have made an observation regarding liaising with

others and obtaining assurance under risk 1 regarding risk management.

| No. | Observation and Implications | Impact / Priority | Management response and action plan including responsible officer | |
|---|---|---|---|---|
| 3.1 | **Logotech -** The current link to access Logotech uses Internet Explorer which stopped receiving support/security updates from June 25, 2022.<br><br>As Internet Explorer is unsupported, there are no continued security updates for this browser. We advise to liaise with ICT (and the supplier if necessary) to arrange for Logotech to be accessed via a newer, supported, browser. | High | **Agreed.** | |
| | | | Responsible Officer: Charlotte Thompson | Target Date:31.03.23 |
| 3.2 | **PP -** Access to Altair (Ping and MSS Inclusive) - There are no password deny lists. Password deny lists help/reduce the risk of a brute-force attack, gaining unauthorised access to the system because it removes the possibility of using easy to guess unsecure passwords.<br><br>Resources such as the suggested password deny list from the NCSC provide the top 100k easily guessed passwords that are available in the public domain and therefore these passwords should not be used within any organisation.<br><br>Furthermore, the Pensions Regulator's draft single Code of Practice does place emphasis on cyber security and therefore, the Pensions Regulator advise that pension schemes should seek appropriate information and guidance on cyber security threats (such as that provided by the National Cyber Security Centre), to enhance their ability to respond to, and recover from, cyber incidents. | Medium | **Agreed.** | |
| | | | Responsible Officer: Rachel Lamb / Alexander Thompson | Target Date: 01/05/2023 |
| 3.3 | **PP -** Currently, there is no documented process in place to ensure that users of third-party accounts (Audit account for example) only have access to that account for the prescribed period of time in Altair.<br><br>Without this control, the user of the third-party account could have access to Altair for a longer period of time than required, increasing the risk of a security incident. | Medium | **Agreed.** | |
| | | | Responsible Officer: Rachel Lamb / Alexander Thompson | Target Date: 01/05/2023 |

| | | | | |
|---|---|---|---|---|
| 3.4 | **PP -** There were a high number of user accounts that had been allocated with the 'Manager' role. This role could be used to create a user account on Altair. Internal Audit were advised that this level of access was required to allow staff to complete their operational tasks. NCSC guidance advise to enforce principle of least privilege.<br><br>Peninsula Pensions should carry out a review of the 21 user accounts that are assigned 'manager role', and establish whether these are appropriate and necessary for their operational tasks.<br><br>Furthermore, Peninsula Pensions should also carry out a review that all user accounts comply to the concept of "least privilege". A record of these checks should be maintained. | Medium | **Agreed.**<br><br>Responsible Officer: Rachel Lamb / Alexander Thompson | Target Date: 01/05/2023 |
| 3.5 | **PP -** There is no documented policy/procedural document which specifically details the creation and approval process for new users of Altair (Ping and MSS account inclusive).<br><br>By having a standardised procedure in place, it ensures consistency and clarity of new users being added to the Altair solution (Ping and MSS account inclusive). | Low | **Agreed** – checklist to be considered re ALTAIR.<br><br>Responsible Officer: Rachel Lamb / Alexander Thompson | Target Date: 01/05/2023 |
| 3.6 | **PP & Logotech** - There are no documented process/ guidance notes/Standard Operating Procedure regarding the closure of user accounts when they are no longer required for either Altair or Logotech.<br><br>With regards to business continuity, there is a risk that Officers leave (or are away from) the organisation and that processes are not known leading to a user account not being removed as expected. | Low | DPF – **Agreed.** Will develop a leavers checklist for the investment team which will include an action to delete user from Logotech.<br><br>Responsible Officer: Charlotte Thompson<br><br>PP – **Agreed.** – checklist to be considered re ALTAIR.<br><br>Responsible Officer: Rachel Lamb / Alexander Thompson | Target Date: 01/07/2023<br><br>Target Date: 01/05/2023 |
| 3.7 | **PP -** It was established from a discussion with the Systems Development Manager (Pensions) that there were three user accounts that were 'MSS Content Admins' who would not be expected to be.<br><br>By incorporating this check into the quarterly review of user accounts would ensure that access to systems controlled by Altair access is appropriate. | Low | **Agreed.**<br><br>Responsible Officer: Rachel Lamb / Alexander Thompson | Target Date: 01/05/2023 |

| | | | | |
|---|---|---|---|---|
| 3.8 | The NCSC guidance advises against enforced password changes on a periodic basis. Consideration should be given to investigating whether the requirement to periodically change passwords in both Altair and Logotech can be disabled. This would support users maintaining a more complex password in line with NCSC advise of having a three random word combination as a password e.g. 'purpleclockcat'.<br><br>Current NCSC guidance recommends not enforcing password changes but reducing reliance on passwords through the use of MFA, and the use of technical controls. (https://www.ncsc.gov.uk/collection/passwords/updating-your-approach) | Low | DPF - Logotech does not require users to periodically change their passwords. | |
| | | | Responsible Officer: Charlotte Thompson | Target Date: Complete. |
| | | | PP – **Agreed.** | |
| | | | Responsible Officer: Rachel Lamb / Alexander Thompson | Target Date: 01/05/2023 |
| 3.9 | **Logotech -** The extent of user access logs, as confirmed by the Investment Manager, is that it shows when a user has last logged on. Despite Logotech being a relatively low-risk system, as it does not hold personal data, general best practice is to have logging and monitoring enabled/in place to ensure only authorised personnel have access to the system. It is noted that the number of authorised users that have access to Logotech is limited to the minimum necessary, with only two people being allowed onto the system at once.<br><br>The Investment Manager should establish with the supplier if there are any further logs available for access to Logotech to enable periodic review to ensure only authorised users have accessed the system/data. | Low | **Agreed.** Will contact Logotech and ask the question. | |
| | | | Responsible Officer: Charlotte Thompson | Target Date: 31.03.23 |
| 3.10 | **PP -** There are generic/shared accounts used to access Altair; auditscc, devaudit, and swapaudit account as examples. These accounts are not attributable to an individual within the system. Current best practice is that generic/shared user accounts should be avoided where possible.<br><br>Management should establish a process to manage the audit generic user accounts in a manner that assigns it to a specific user. This would provide a better audit trail of access within the system. | Low | **Agreed.** | |
| | | | Responsible Officer: Rachel Lamb / Alexander Thompson | Target Date:01/05/2023 |

| | | | | |
|---|---|---|---|---|
| 3.11 | **PP -** The authentication method currently requires two pieces of knowledge (rather than something you know and have, for example, a password and a one-time password) to access the site, and there is the potential for this information to be acquired by an adversary, thus gaining unauthorised access to their account.<br><br>Liaising with the suppler could identify additional measures to further secure the MSS accounts, for example, the use of a one-time password. | Opportunity | **Agreed.** The new version of MSS, which we will implement January 2023, has this feature built in. | |
| | | | Responsible Officer: Rachel Lamb / Alexander Thompson | Target Date: 01/05/2023 |

| **4. Risk Area: Poor user understanding of cyber-risk and security procedures results in the disclosure of information (Training).** | **Level of Assurance** |
|---|---|
| | **Limited Assurance** |

**Opinion Statement:**

Our most recent Cyber Security audits of DCC have found training materials are made available to staff. It was confirmed that training materials were comprehensive, covering current and hot topics. The training available is delivered using different learning styles, including videos, reading, and interactive e-learning modules. Additionally, the Strategic Cyber Security Manager releases regular guidance via the staff newsletter and more in-depth articles on Inside Devon which is accessible by Pensions staff.

Devon County Council (DCC) have a framework of security policies and procedures. Part of this framework includes mandatory Cyber Awareness Training and the Personal Information Security Policy, which requires mandatory acknowledgement alongside the training. However, even with the training being mandatory, not all staff employed by Peninsula Pensions and Devon Pension Fund, or DCC Pension Board and Committee members, have completed this training. The details of compliance with the mandatory training are detailed in the observations below.

Pensions Administration Standards Association (PASA) recommend having a cyber security policy. Peninsula Pensions have recently, October 2022, developed a Cyber Security Policy. This policy document makes reference to the relevant DCC Policies already in place. It includes details of roles and responsibilities in relation to Cyber Security and provides links to key supplier assurance certifications. The draft Policy is awaiting agreement from the Investment Team and approval by the Pensions Board and Senior Management.

| No. | Observation and Implications | Impact / Priority | Management response and action plan including responsible officer |
|---|---|---|---|
| 4.1 | Not all staff from Devon Pension Fund & Peninsula Pensions have completed their mandatory cyber security related e-learning | High | DPF - **Agreed** to ensure all training to be completed |

and Personal Information Security Policy acknowledgement on MetaCompliance.

Staff who are untrained or who have not completed a recent refresher in cybersecurity are more likely to cause and/or enable security breaches. Below shows a summary table of Officers who have **NOT** completed the DCC mandatory Cyber Security related training:

| DPF Operational Teams (No. of Staff) | Cyber Security Awareness Training | Personal Information Security Policy |
|---|---|---|
| DCC Investments Team (6) | 33% | 17% |
| Peninsula Pensions (72) | 17% | 29% |

| | | | |
|---|---|---|---|
| | | | Responsible Officer: Charlotte Thompson / Target Date:31.03.23 |
| | | | PP - **Agreed** - Emails have since been sent to individuals now we have the meta compliance data – requested from DPO team that Managers automatically notified if staff have not actioned after a set period of time. |
| | | | Responsible Officer: Rachel Lamb / Alexander Thompson / Target Date:31.03.23 |
| 4.2 | Not all DCC Board / Committee members have completed their mandatory cybersecurity training. | High | **Agreed.** Contacted Karen Strahan who will follow this up. |
| | Without specific knowledge around cyber security, it opens the possibility that the board cannot deliver the scrutiny aspects of the boards role when reviewing the risk registers in their meetings. | | Responsible Officer: Charlotte Thompson / Target Date:31.03.23 |
| 4.3 | Non-DCC Board/Committee members do not complete any cyber related training.<br>Without specific knowledge around cyber security, it opens the possibility that the board cannot deliver the scrutiny aspects of | Medium | **Agreed.** Will investigate covering this topic at future board/committee training sessions |

| Name | Cyber Security Training | PISP acceptance |
|---|---|---|
| CS | Not started | Not completed |
| GG | Not started | Not completed |
| HG | Not started | Not completed |
| JM | Not started | Not completed |
| MH | Not started | Not completed |
| PB | 2021-11-02 | Not completed |
| SRJ | 2021-11-09 | 2021-11-09 |
| YA | Not started | Not completed |

| | | | | |
|---|---|---|---|---|
| | the boards role when reviewing the risk registers in their meetings. | | Responsible Officer: Charlotte Thompson | Target Date:31.03.23 |

| **5. Risk Area: Devon County Council (DCC) recovery processes fail following a cyber-attack or IT disruption (Devon Pension Fund and Peninsula Pensions BC & DR plans).** | **Level of Assurance** |
|---|---|
| | **Limited Assurance** |

**Opinion Statement:**

Our review established that the DCC Investments Team and Peninsula Pensions both have service area Business Continuity Plans (BCP) in place to ensure that there is a plan to continue delivery and restore business as usual services when misfortune or an incident occurs. Both BCPs use the Devon Emergency Planning Service (DEPS) template, were up-to-date, and had been updated within the previous six months. Within the template, there is specific reference to a cyber-attack/ IT disruption as an event which could require activation of the BCP. However, improvements can be made to the BCPs for both the DCC Investment team and Peninsula Pensions. Our observations are recorded below.

Currently Devon County Council (DCC) ICT Business Continuity/Disaster Recovery (BCP/DR) plans are not fit for purpose as identified in the DCC Corporate Risk Register. However, Peninsula Pensions have contingencies in place to ensure continuity of services, including accessing Altair, without DCC network infrastructure. Peninsula Pensions are able to obtain limited licenses that would allow users/officers to work from home. The Investments Team BCP identifies that investments can place transfers over the phone. But there is no detail regarding how the absence of the data and functionality that Logotech provides will be managed.

The DEPS BCP template requires a prioritisation of business-critical services that need to be restored to resume business as usual. Within each section, the Recovery Time Objective (RTO; the targeted duration of time and a service level within which a business process must be restored after a disaster.) is stated, but the Recovery Point Objective (RPO; maximum tolerable period in which data might be lost from an IT service due to a major incident.) is not.

There has been no testing of Devon Pension Fund's or Peninsula Pension's BCP within the past year, nor is there a scheduled plan to test.

The BCP for DPF was reviewed as part of the Treasury Management audit, and it was highlighted that some details are out of date. This review had further tested and highlighted the below observations.

| No. | Observation and Implications | Impact / Priority | Management response and action plan including responsible officer | |
|---|---|---|---|---|
| 5.1 | There is no scheduled testing for the Investments Team's nor PP's BCP, and there has not been a test completed within the past 12 months.<br>Testing a BCP is a vital to ensure that the plan is adequate to | High | DPF - **Agreed**, will seek a meeting with Keith Reed/DAP to work on a plan to test the BCP. | |
| | | | Responsible Officer: Rachel Lamb / Alexander Thompson | Target Date: 01/07/2023 |

| | | | | |
|---|---|---|---|---|
| | deal with any event that can cause disruption to a service.<br>A specific Cyber BC exercise should be completed regularly to ensure plans are effective. | | PP - **Agreed.** Peninsula Pensions Senior Management Team invoked the BCP during COVID-19 which proved extremely successful during this 'real' time event, and there were contingency plans in place to cover the whole team as necessary. | |
| | | | Responsible Officer: Charlotte Thompson | Target Date:31.03.2023 |
| 5.2 | Recovery Point Objective (RPO), t*he point in time to which data must be recovered after an outage,* is not outlined within either of the BCP's. By having a RPO defined, it gives a clear point in time to which data must be recovered after an outage.<br>It is acknowledged that the BCP's are DCC Corporate Forms and do not specify a requirement for this to be recorded. It would be beneficial to liaise/work with the Emergency Planning and ICT to seek SME advice and guidance on how to incorporate this into the BCP's. | High | DPF – **Agreed.** | |
| | | | Responsible Officer: Charlotte Thompson | Target Date: 31.03.2023 |
| | | | PP - **Agreed.** | |
| | | | Responsible Officer: Rachel Lamb / Alexander Thompson | Target Date: 01/05/2023 |
| 5.3 | We have reviewed the BCP's for PP and DCC Investments Team and we have identified a number of areas where improvements can be made. | High | DPF - **Agreed.** | |
| | | | Responsible Officer: Charlotte Thompson | Target Date:31.03.2023 |

| | | | |
|---|---|---|---|
| | **DCC Investments Team BCP**<br>- Reference made to DCC Finance BCP but no copy held (furthermore Finance BCP does not include reference to online banking which is key system for investments team).<br>- Not all of the DEPS template is complete (Key contact section does not include supplier contact details for example).<br>- We understand that Logotech is used to help compile the cashflow position - the BCP does not include detail of how this will be mitigated to enable continued operations.<br>- No plan to implement a direct internet connection with MFA for limited users to Logotech if DCC network not available - (this has been explored and incorporated as an option by PP for Altair).<br>- Inclusion of aspects that are not relevant to the Investment teams operations e.g., Payment of staff - this is the function of the HR/Payroll department.<br><br>**PP BCP**<br>- Links within the document are not available (Page 11, Altair link)<br><br>The need for accurate documentation in relation to BCP can be the difference between a successful conclusion to an event or a disaster. Everyone must have the same understanding and expectation of response. To ensure robustness both BCP's should be reviewed and updated, as necessary. | | PP - **Agreed**, links will be updated.<br><br>Responsible Officer: Rachel Lamb / Alexander Thompson — Target Date: 01/05/2023 |
| 5.4 | Management were not able to confirm that the backups administered by the third-party suppliers are off-line (air gapped) and immutable (not able to be altered).<br><br>The impact of a cyber-attack can be significantly reduced if backups are off-line and/or not able to be altered.<br><br>DPF/PP would benefit from their third-party providers having these technical controls in place. This would also be in line with current NCSC advice and the DCC preferred approach. | Medium | DPF – **Agreed.** Will contact Logotech and Brunel.<br><br>Responsible Officer: Charlotte Thompson — Target Date: 31.03.23<br><br>PP – **Agreed.** We can confirm that Heywood back up Altair and the backup is 'not to be altered' / offline on a backup system. Heywood's have obtained the recognised ISO / Cyber Essentials which would recognise these areas as requirements.<br><br>Responsible Officer: Rachel Lamb / Alexander Thompson — Target Date: Completed. |

| | | | | |
|---|---|---|---|---|
| 5.5 | Historically the BCP's have not been required to be reviewed and approved by the Board/Committee.<br><br>In order for the Board to effectively review and scrutinise the risk registers, key documents relating to the mitigating controls, e.g. BCP's, could also be made available to the Board in order for the controls to be reviewed as well.<br><br>There is no record/note in the PP risk register or on either BCP stating that it has been reviewed by a second party e.g. Emergency Planning Team. | Low | DPF - **Agreed**, will take it to the pension board. | |
| | | | Responsible Officer: Charlotte Thompson | Target Date: July 2023 |
| | | | PP - **Agreed**. The Board and Committee would not necessarily have the required understanding/knowledge relating to the pension administration system to be able to provide advice on this area, hence historically no approval sought at this level. The BCP is held centrally where the Emergency Planning Team are able to view however. | |
| | | | Responsible Officer: Rachel Lamb / Alexander Thompson | Target Date: July 2023. |

## Scope and Objectives

The Objective of the audit is to evaluate Devon Pension Funds control framework in relation to Cyber Security, using the Pensions Regulator's cyber security principles to provide assurance that cyber risks are being effectively managed.

The key risks *(and control areas)* that this audit will consider are:

- Risks are not identified to mitigate against threats to the IT infrastructure *(Risk Management).*
- Suppliers or partners disclose information or disrupt the pension service *(Supply Chain Management).*
- Unauthorised modification or deletion of data *(Altair and Logotech access controls)*
- Poor user understanding of cyber-risk and security procedures results in the disclosure of information *(Training).*
- Devon County Council (DCC) recovery processes fail following a cyber-attack or IT disruption *(Devon Pension Fund and Peninsula Pensions BC & DR plans).*

The risks above encompass a significant proportion of the Pensions Regulators cyber security principles.

Devon Pension Fund and Peninsula Pensions IT infrastructure is not segmented from the Main DCC ICT environment and therefore reliance will also be placed on the DCC Cyber security audit work already carried out.

## Inherent Limitations

The opinions and recommendations contained within this report are based on our examination of restricted samples of transactions / records and our discussions with officers responsible for the processes reviewed.

## Confidentiality under the National Protective Marking Scheme

This report is protectively marked in accordance with the National Protective Marking Scheme. It is accepted that issues raised may well need to be discussed with other officers within the Council, the report itself should only be copied/circulated/disclosed to anyone outside of the organisation in line with the organisation's disclosure policies. This report is prepared for the organisation's use. We can take no responsibility to any third party for any reliance they might place upon it.

| Marking | Definitions |
|---|---|
| Official | The majority of information that is created or processed by the public sector. This includes routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened threat profile. |
| Official: Sensitive | A limited subset of OFFICIAL information could have more damaging consequences if it were lost, stolen or published in the media. This subset of information should still be managed within the 'OFFICIAL' classification tier but may attract additional measures to reinforce the 'need to know'. In such cases where there is a clear and justifiable requirement to reinforce the 'need to know', assets should be conspicuously marked: 'OFFICIAL–SENSITIVE'. All documents marked OFFICIAL: SENSITIVE must be handled appropriately and with extra care, to ensure the information is not accessed by unauthorised people. |

## Definitions of Audit Assurance Opinion Levels

| Assurance | Definition |
|---|---|
| Substantial Assurance | A sound system of governance, risk management and control exists, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited. |
| Reasonable Assurance | There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified which may put at risk the achievement of objectives in the area audited. |
| Limited Assurance | Significant gaps, weaknesses or non-compliance were identified. Improvement is required to the system of governance, risk management and control to effectively manage risks to the achievement of objectives in the area audited. |
| No Assurance | Immediate action is required to address fundamental gaps, weaknesses or non-compliance identified. The system of governance, risk management and control is inadequate to effectively manage risks to the achievement of objectives in the area audited. |

## Definition of Observation Priority

| | |
|---|---|
| High | A significant finding. A key control is absent or is being compromised; if not acted upon this could result in high exposure to risk. Failure to address could result in internal or external responsibilities and obligations not being met. |
| Medium | Control arrangements not operating as required resulting in a moderate exposure to risk. This could result in minor disruption of service, undetected errors or inefficiencies in service provision. Important observations made to improve internal control arrangements and manage identified risks. |
| Low | Low risk issues, minor system compliance concerns or process inefficiencies where benefit would be gained from improving arrangements. Management should review, make changes if considered necessary or formally agree to accept the risks. These issues may be dealt with outside of the formal report during the course of the audit. |
| Opportunity | An observation to drive operational improvement which may enable efficiency savings to be realised, capacity to be created, support opportunity for commercialisation / income generation or improve customer experience. These observations do not feed into the assurance control environment. |

## Devon Audit Partnership

The Devon Audit Partnership has been formed under a joint committee arrangement comprising of Plymouth, Torbay, Devon, Mid Devon, South Hams & West Devon, Torridge and North Devon councils. We aim to be recognised as a high-quality internal audit service in the public sector. We work with our partners by providing a professional internal audit service that will assist them in meeting their challenges, managing their risks and achieving their goals. In carrying out our work we are required to comply with the Public Sector Internal Audit Standards along with other best practice and professional standards. The Partnership is committed to providing high quality, professional customer services to all; if you have any comments or suggestions on our service, processes or standards, the Head of Partnership would be pleased to receive them at tony.d.rose@devon.gov.uk

# Internal Audit Report - Final
## Peninsula Pensions
## Pensions ESCROW Account

March 2023

devon audit partnership
Auditing for Achievement

| Service Objective |
|---|
| To ensure unclaimed refunds of contributions are moved out of the Fund before the 5 year mark, so as to not incur unauthorised payment charges or sanctions. |
| **Audit Opinion** |
| **Substantial Assurance** - A sound system of governance, risk management and control exists, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited. |

| Assurance Opinion on Risks or Areas Covered<br>- key concerns or unmitigated risks | Level of Assurance |
|---|---|
| **The Account is not being maintained in accordance with regulatory requirements, resulting in inaccurate, ineligible, untimely, duplicate, or fraudulent payments being made from the account.** | **Substantial Assurance** |
| *These areas / risks combine to provide the overall audit assurance opinion. Definitions of the assurance opinion ratings can be found in the Appendices. The observations and findings in relation to each of these areas has been discussed with management, see the "Detailed Audit Observations and Action Plan" appendix A. This appendix records the action plan agreed by management to enhance the internal control framework and mitigate identified risks where agreed* | |

## Introduction

When a member leaves the Pension fund after the first 3 months of employment, but before the two year vesting period, they are entitled to a refund of their pension contributions, which they must apply for to allow the Fund to issue the payment. Under certain conditions, if the refund is not issued within 5 years, the payment may be subject to an Unauthorised Payments Charge of 40% (member), Unauthorised Payments Surcharge of 15% (member), and Scheme Sanction Charge of 40% (administering authority).

Guidance issued from the Local Government Association states that 'Administering Authorities may instead discharge liability by paying the refund to an ESCROW account before the expiry of five years. The Head of Pensions at the time set up an Escrow account for this purpose in 2019, and the Finance Manager took on the administration of the payment process, including setting up the ability to make payments on FINEST.

As of November 2022, the balance of the Escrow account stood at £539,358.37.

## Executive Summary

There are effective and efficient controls in place to ensure that unclaimed refunds of contributions and death grants are moved out of the Fund prior to reaching an age that they attract unauthorised payment charges and sanctions, the account is monitored and reviewed regularly, and payments made are accurate and not duplicate or fraudulent.

The Finance Manager maintains a spreadsheet detailing all payments that have been moved across into the account, and all payments that have been made from the account. The bank statements for the account are reviewed and authorised by both the Finance Manager and the Pensions Technical Manager.

We reviewed a sample containing both refunds and death benefits paid out, and refunds and death benefits still held in the account. We found that all payments made were accurate, timely and that records had been maintained to ensure there could be no duplication. All payments still in the account were found to be accurate with adequate supporting documentation.

If you would like a meeting to discuss the report, this should be arranged with Pandora Saxby (pandora.saxby@devon.gov.uk).

## Issues for the Annual Governance Statement

The evidence obtained in internal audit reviews can identify issues in respect of risk management, systems and controls that may be relevant to the Annual Governance Statement.

This review has not identified any issues that may be relevant to the Annual Governance Statement.

## Acknowledgements

We would like to express our thanks and appreciation to all those who provided support and assistance during the course of this audit.

**Tony Rose**
**Head of Partnership**

## Detailed Audit Observations and Action Plan

| Risk 1: The Account is not being maintained in accordance with regulatory requirements, resulting in inaccurate, ineligible, untimely, duplicate, or fraudulent payments being made from the account.: | Level of Assurance<br>Substantial Assurance |
|---|---|

**Opinion Statement:**
There is sufficient documentation in place to detail the process for making payment of refunds from the Escrow account and the associated legislation.

The Escrow account is monitored by way of a spreadsheet that is maintained by the Finance Manager. The spreadsheet is suitably located, and access appropriately controlled.

The spreadsheet records details of all payments moved from the fund into the Escrow account, as well as bank statements and payments out. The Escrow account transactions are reviewed and authorised on a monthly basis. The bank statements are checked and signed by the Finance Manager and then sent to the Pensions Technical Manager to be countersigned.

We reviewed a sample of 10 refunds paid from the Escrow account. All payments were made in a timely manner upon receipt of the refund form, the monitoring spreadsheet was updated accordingly, and the refund recipient's Altair record was updated to show that they had exited the fund and there was no further liability.

An annual task is carried out to identify refunds approaching 5 years of age and move these out of the Fund and into the Escrow account. We reviewed a sample of refunds held in the Escrow account and confirmed that the amounts moved across were accurate and matched the refund calculation.

| No. | Observation and Implications | Impact / Priority | Management response and action plan including responsible officer |
|---|---|---|---|
| No observations and recommendations recorded | | | |

## Scope and Objectives

The objective of this audit was to provide assurance that the ESCROW account is being maintained / managed in accordance with the Pension Regulations and that the control framework is effective and adequate.

## Inherent Limitations

The opinions and recommendations contained within this report are based on our examination of restricted samples of transactions / records and our discussions with officers responsible for the processes reviewed.

## Confidentiality under the National Protective Marking Scheme

This report is protectively marked in accordance with the National Protective Marking Scheme. It is accepted that issues raised may well need to be discussed with other officers within the Council, the report itself should only be copied/circulated/disclosed to anyone outside of the organisation in line with the organisation's disclosure policies. This report is prepared for the organisation's use. We can take no responsibility to any third party for any reliance they might place upon it.

| Marking | Definitions |
|---|---|
| Official | The majority of information that is created or processed by the public sector. This includes routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened threat profile. |
| Official: Sensitive | A limited subset of OFFICIAL information could have more damaging consequences if it were lost, stolen or published in the media. This subset of information should still be managed within the 'OFFICIAL' classification tier but may attract additional measures to reinforce the 'need to know'. In such cases where there is a clear and justifiable requirement to reinforce the 'need to know', assets should be conspicuously marked: 'OFFICIAL–SENSITIVE'. All documents marked OFFICIAL: SENSITIVE must be handled appropriately and with extra care, to ensure the information is not accessed by unauthorised people. |

## Definitions of Audit Assurance Opinion Levels

| Assurance | Definition |
|---|---|
| Substantial Assurance | A sound system of governance, risk management and control exists, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited. |
| Reasonable Assurance | There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified which may put at risk the achievement of objectives in the area audited. |
| Limited Assurance | Significant gaps, weaknesses or non-compliance were identified. Improvement is required to the system of governance, risk management and control to effectively manage risks to the achievement of objectives in the area audited. |
| No Assurance | Immediate action is required to address fundamental gaps, weaknesses or non-compliance identified. The system of governance, risk management and control is inadequate to effectively manage risks to the achievement of objectives in the area audited. |

## Definition of Observation Priority

| | |
|---|---|
| High | A significant finding. A key control is absent or is being compromised; if not acted upon this could result in high exposure to risk. Failure to address could result in internal or external responsibilities and obligations not being met. |
| Medium | Control arrangements not operating as required resulting in a moderate exposure to risk. This could result in minor disruption of service, undetected errors or inefficiencies in service provision. Important observations made to improve internal control arrangements and manage identified risks. |
| Low | Low risk issues, minor system compliance concerns or process inefficiencies where benefit would be gained from improving arrangements. Management should review, make changes if considered necessary or formally agree to accept the risks. These issues may be dealt with outside of the formal report during the course of the audit. |
| Opportunity | An observation to drive operational improvement which may enable efficiency savings to be realised, capacity to be created, support opportunity for commercialisation / income generation or improve customer experience. These observations do not feed into the assurance control environment. |

## Devon Audit Partnership

The Devon Audit Partnership has been formed under a joint committee arrangement comprising of Plymouth, Torbay, Devon, Mid Devon, South Hams & West Devon, Torridge, and North Devon councils. We aim to be recognised as a high-quality internal audit service in the public sector. We collaborate with our partners by providing a professional internal audit service that will assist them in meeting their challenges, managing their risks, and achieving their goals. In conducting our work, we are required to comply with the Public Sector Internal Audit Standards along with other best practice and professional standards. The Partnership is committed to providing high quality, professional customer services to all; if you have any comments or suggestions on our service, processes or standards, the Head of Partnership would be pleased to receive them at tony.d.rose@devon.gov.uk