Public Document Pack

Havering
LONDON BOROUGH

LOCAL PENSION BOARD
AGENDA

4.00 pm	**Tuesday 29 March 2022**	**Zoom**

Members 4: Quorum 2

Mark Holder, Scheme Member Representative
Yasmin Ramjohn, Scheme Member Representative
Dionne Weekes, Scheme Memebr Representative

Denise Broom, Scheme Employer Representative
Andrew Frater, Scheme Employer Representative

For information about the meeting please contact:
Luke Phimister 01708 434619
luke.phimister@onesource.co.uk

AGENDA ITEMS

1 CHAIR'S ANNOUNCEMENTS

The Chair will announce details of the arrangements in case of fire or other events that might require the meeting room or building's evacuation.

2 APOLOGIES FOR ABSENCE

(if any) – receive.

3 DISCLOSURE OF INTEREST

Members are invited to disclose any interest in any items on the agenda at this point of the meeting.

Members may still disclose any interest in an item at any time prior to the consideration of the matter.

4 MINUTES OF THE MEETING (To Follow)

To approve as correct the minutes of the meeting held on 8 February 2022 (to follow) and authorise the Chair to sign them.

5 TO RECEIVE FEEDBACK FROM RECENT MEETINGS OF THE PENSIONS COMMITTEE (Verbal Report)

6 ANNUAL INTERNAL CONTROL ASSURANCE REPORT (Pages 1 - 46)

Report attached and appendix attached.

7 CYBER SECURITY ASSURANCE STATEMENT - RESPONSE TO QUESTIONS FROM LAST MEETING (Pages 47 - 48)

Report attached.

8 PENSIONS BOARD VACANCIES (Verbal Report)

Zena Smith
Democratic and Election Services Manager

LPP

Local Pensions Partnership
Administration

Annual Internal Control Assurance Report 2020/21

for the year ending 31st March 2021

August 2021

lppapensions.co.uk

Contents

03 Executive Summary

06 Report by the Head of Risk & Compliance

09 LPPA Structure

12 Control Environment

16 Control Objectives

19 Control Testing

21 Overview of Internal Audit Activity 2021/21

24 Overview of LPPA Risk & Compliance Activity 2020/21

36 Accreditations

EXECUTIVE SUMMARY

LPPA, part of the LPP Group, provides pension administration services to over 600,000 members across 1,900 employers for its 17 LGPS and blue light clients.

We deliver high-quality pensions administration services to Local Government, Police and Firefighters Pension Schemes.

EXECUTIVE SUMMARY

From the formation of LPP Group in 2016, our Pension Administration activity was managed within LPP Group (the parent company). When we formed LPP, alongside LPPI (our Investment and separate subsidiary business) we also formed the LPP Administration (LPPA) subsidiary, which had been largely dormant since. We operated with a large overlap in our Executive and Non-Executive management structures. In 2019, we decided that the best way to enable both operating businesses to flourish in the years ahead is to provide both with a similar level of focussed and independent management whilst maintaining the overarching support of the wider LPP Group. By creating focused business unit management, contained within the wider LPP capabilities, we felt able to ensure we calibrate our activities, focussing on what matters for each business unit whilst not losing the DNA that runs through LPP Group.

In June 2020, we re-formed the LPPA subsidiary, and the LPPA Board which is accountable to the LPP Board. All pensions administration staff were TUPE'd across to LPPA along with staff aligned to pensions administration in support functions such as Risk and Compliance, Finance, HR, IT and Change.

The Covid-19 pandemic created additional pressures for LPPA including unplanned peaks in some operational teams (e.g. bereavements) and new opportunities. It has accelerated the move to a more agile working environment for LPPA with all staff having the flexibility to decide, dependent on business needs, whether they return to the office in Preston or continue to work some days from home. LPPA took the decision to close its two satellite offices in Hertford and Havering with all staff moving to be permanent home workers. The pandemic has proved that flexible working can be beneficial in achieving a good work-life balance, without having any adverse impact on the services we provide.

EXECUTIVE SUMMARY

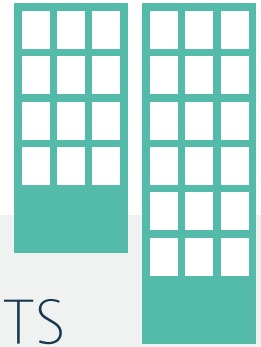
This Report outlines the specific control objectives to support the evolution of LPPA as we move forward into the future.

LPPA's aim is to make pensions simple at a time when our members need us the most. Our scale gives us insight, which puts us in a great place to do more and do it better to be the best public sector pensions administration provider.

We are proud to provide first-class, end-to-end pensions administration services including payroll, and member and employer engagement. Our service consistently exceeds Service Level Agreements and we take a proactive approach to improving administration services across the sector, striving to become a pensions administration Centre of Excellence.

During the year 2020/21 we have developed further the strong, effective and collaborative working relationships we have with our clients. Our focus on member experience combined with working constructively with our clients and their employers enables us to drive continuous improvement in the services we offer.

1
OFFICE



17
CLIENTS

1,900
EMPLOYEES

600,000
MEMBERS

REPORT BY THE HEAD OF RISK & COMPLIANCE

This Report relates to the pensions administration services provided by Local Pensions Partnership Administration Limited (LPPA).

REPORT BY THE HEAD OF RISK & COMPLIANCE

Janet Morville-Smith
Head of Risk & Compliance LPPA

In addition to the Covid-19 pandemic, an awful lot has happened during 2020/21 with the establishment of a dedicated Risk & Compliance function within the pensions administration business, and the restructure of the LPP Group. And if that wasn't enough, we also started the mammoth task of transitioning over to a new administration system (Project PACE).

Since June 2020, LPPA has come a very long way in a very short space of time. We have engaged with our staff to drive our corporate values and behaviours into everything we do and I am proud of the way our people have embraced the changes and challenges that have been thrown at them and their resolve and dedication to make LPPA the best pension administration service provider in the public sector is a testament to them.

My Quality Assurance & Compliance Monitoring team have done some exceptional work this year reviewing and testing the quality and controls in place across many areas of LPPA. Their programme of work will span the whole of the business over the coming months.

In 2020/21 the team have performed 14 compliance monitoring reviews which have identified areas where we can drive improvements in processes, practices and understanding. Inconsistencies in the operation of processes and documentation across our 17 clients were high on our list of findings, and is on the agenda to streamline as part of Project Pace.

REPORT BY THE HEAD OF RISK & COMPLIANCE

The introduction of compliance monitoring into LPPA has enabled us to assess the efficiency and effectiveness of the activities LPPA perform on behalf of our clients and drive continuous improvements in the services we provide and ultimately to enhance the member experience.

From the evidence provided by my team, Deloitte, client auditors and my own involvement within the business, I can provide full assurance to all clients who have used the pensions administration services that those services are being delivered by LPPA in compliance with the Pension Regulator's Code of Practice 14 and local government and public sector pensions legislation. In addition, I can confirm that those services are being delivered in compliance with the UK data protection and information security requirements.

This report will not omit or distort information relevant to the scope of the services being described in the Control Objectives, whilst acknowledging that it has been prepared to meet the common needs of a broad range of clients and may not therefore include every aspect of the services that each individual client may consider important in its own particular environment.

LPPA STRUCTURE

LPPA STRUCTURE

Organisational Structure

LPPA is a subsidiary of Local Pensions Partnership Limited. LPPA's head office is based in Preston and operates with staff who are either based in our Preston office, or are permanent home workers.

LPPA

LPPA provides pension administration services to LGPS Funds and other public sector schemes. We look after the needs of over 600,000 pension scheme members across a variety of schemes and industries.

As a leading third party pensions administrator, we are responsible for the pension administration services, including calculation and payment of pension benefits, data quality and member and employer engagement.

Internal Controls

The system of internal controls is based upon an ongoing process designed to identify the risks to the achievement of policies, aims and objectives; to evaluate the nature and extent of those risks; and to manage them efficiently, effectively and economically.

A key element of this structure includes formally agreed, clear definitions of the responsibilities and authority delegated to individual managers across all major activities, supported by LPPA's Senior Leadership Team and the LPPA Board.

The LPPA Risk Management Framework includes the Risk Register, which maps and monitors the risks that threaten achievement of the Control Objectives and regularly reviews and tests the Controls to ensure they remain effective in managing those risks.

Governance Structure

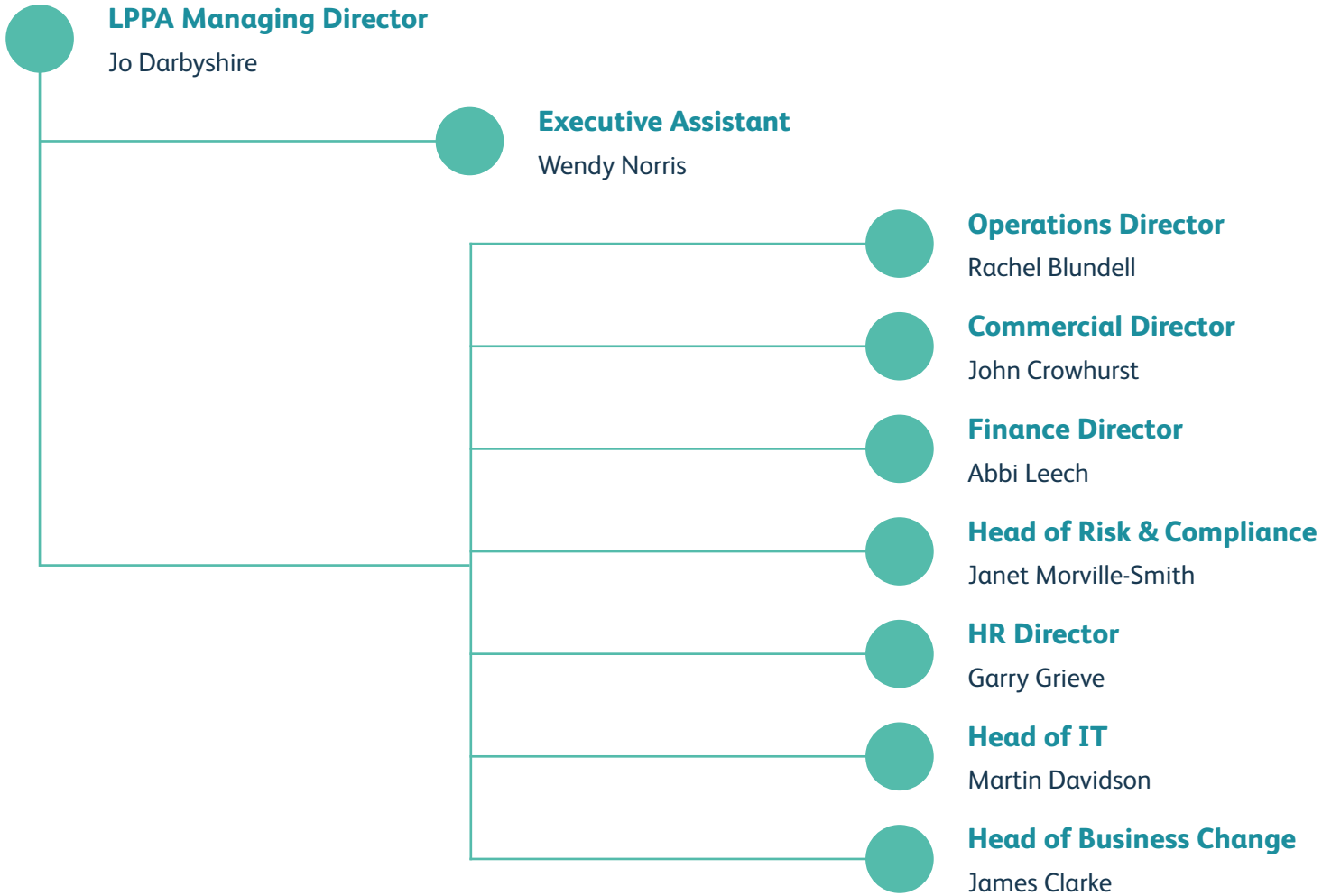
The LPPA Board is chaired by Sir Peter Rogers and includes 4 Non-Executive Directors.

The LPPA Senior Leadership Team is led by Jo Darbyshire, LPPA Managing Director, and includes Senior Executives with the appropriate skills, knowledge and expertise to achieve the strategic objectives of LPPA.

Jo Darbyshire
LPPA Managing Director

LPPA STRUCTURE

LPPA Senior Leadership Team



CONTROL ENVIRONMENT

The senior leadership team of LPPA are committed to deploying a strong control environment for pension administration services through the following measures.

CONTROL ENVIRONMENT

Risk Management Framework

LPPA operates within a risk management framework. This framework uses a "three lines of defence" model with the administration business supported by a dedicated risk function who provide oversight and co-ordinated reporting to the Senior Leadership Team and the LPPA Board. The Risk Management Framework is responsible for ensuring that business level risks are managed effectively and that mandated policies and controls are in place and operating effectively. This covers the following areas relating to administration:

- ✓ Risk management and reporting
- ✓ Internal and external audits
- ✓ Internal control framework
- ✓ Fraud prevention
- ✓ Business continuity
- ✓ Complaints and errors
- ✓ Data Protection and Information Security

LPPA maintains a comprehensive Risk Register which covers:

- ✓ Strategic risks
- ✓ Operational risks
- ✓ Financial risks
- ✓ Commercial risks
- ✓ Risk & Compliance risks
- ✓ IT risks
- ✓ Change risks
- ✓ HR risks

These risks are reviewed on a regular basis by Risk & Compliance with the relevant business areas. We work with clients to identify and understand the key risks which apply to their schemes and how they interact with our own Risk Register so that we can identify and implement measures to effectively mitigate these risks.

Quality Assurance & Compliance Monitoring

We recognise our responsibilities to ensure that the activities of LPPA and our people are carried out properly and with the utmost propriety, and that our managers conduct their activity properly and in accordance with statutory and regulatory requirements.

To ensure administration activities are carried out competently, LPPA has a dedicated Risk & Compliance function. Integral to this function is maintaining an awareness of the external environment to ensure regulatory and legislative changes which impact us are adequately dealt with in our operations. In support of this objective, we issue a number of corporate procedural and policy documents to our staff, including: Code of Conduct; Confidentiality; Gifts and Hospitality Policy; Anti-Money Laundering Procedures; Data Protection Procedures, Vulnerable Member Policy.

The Quality Assurance & Compliance Monitoring team has implemented a programme of regular quality assurance and compliance monitoring reviews to ensure that our policies, processes and procedures are operating effectively, and they report the results of these to the senior leadership team and the LPPA Board.

Internal Audit

LPPA engaged Deloitte to perform internal audit for FY2020/21.

Compliance & Technical

Our compliance and technical teams work together to assesses the impact of legislative and/or regulatory change which may impact our clients and administration processes. Changes are communicated to staff via technical updates and face-to-face discussions and/or training sessions. LPPA's intranet site is accessible to all administrators and provides a central reference point for technical materials, policies, procedural guidance, standard letter templates and checklists.

Where Government and/or industry bodies publish consultations on proposed legislative change, the compliance and technical teams will carry out an impact assessment and draft responses to the consultation. Where appropriate, the draft responses are shared with our clients and a round-table session is facilitated to discuss the subject matter and share thoughts so that the final response submitted by LPPA is representative of all the relevant stakeholders.

Information Security

Information Security is fundamental to the risk management strategy of the organisation and we take the protection of our information assets and those of our clients very seriously. The Head of IT is responsible for managing IT / information security and has a team of specialists to assist with the management of information security risks across LPPA. LPPA's Data Protection Officer is responsible for monitoring data confidentiality and ensuring compliance with the UK Data Protection Act 2018 and UK GDPR.

The Security Working Group (SWG) is responsible for monitoring Information Security performance on behalf of key stakeholders, and for ensuring that all IT systems and data handling are secured in line with current legislation, industry best practices and ISO 27001 standards.

CONTROL ENVIRONMENT

This is supported by a comprehensive suite of Information Security Management System policies (ISMS), which provide staff with formal guidance on how we protect our information, along with an Annual Information Security and Data Protection Awareness training programme. A range of technical controls are in place to protect our information assets, including next generation firewalls, Security Information and Event Management Software (SIEM), an Intrusion Protection System (IPS) and anti-virus software. These are supported by additional independent Penetration Tests that are carried out by CHECK/CREST approved suppliers. Information Security policies require that users must employ a complex password to access the systems and that they are forced to change their passwords at least every 90 days.

To ensure our service remains highly available and to enhance our business continuity capability, we operate a hosted tier 3 data centre environment with all critical systems and data backed up daily to tape and disk and stored securely off site, ensuring that there are multiple copies of the data available in the event of disruption

All computer systems are only accessible by authorised individuals. All users are assigned a set of unique credentials with access rights that will only allow them access to the information they need to carry out their job function. Access rights for users must be authorised by line managers and specialised technical privileges must be authorised by IT. Access to client databases is further segregated via security groups. Quarterly access reviews of user and privileged access are carried out with the relevant manager / system owner required to review and confirm they are correct.

CONTROL OBJECTIVES

CODE OF PRACTICE 14

1. Accepting clients

- Accounts are set up and administered in accordance with client agreements and applicable regulations.
- Complete and authorised client agreements are operative prior to initiating administration activity.
- Pension schemes taken on are properly established in the system in accordance with the scheme rules and individual elections.

2. Authorising and processing transactions

- Benefits payable and transfer values are calculated in accordance with scheme rules and relevant legislation and are paid on a timely basis.

3. Maintaining financial and other records

- Member records consist of up-to-date and accurate information and are updated and reconciled regularly.
- Contributions and benefit payments are completely and accurately recorded in the proper period.
- Scheme documents (deeds, policies, contracts, booklets) are complete, up to date and securely held.

4. Safeguarding Assets

- Member and scheme data is appropriately stored to ensure security and protection from unauthorised use.
- Funds are safeguarded and payments are suitably authorised and controlled.

5. Monitoring compliance

- Services provided to pension schemes are in line with service level agreements.
- Transaction errors are rectified promptly and Members treated fairly

6. Reporting to clients

- Periodic reports to participants and scheme sponsors are accurate and complete and provided within required timescales.
- Annual reports and accounts are prepared in accordance with applicable law and regulations.
- Regulatory reports are made if necessary.

INFORMATION TECHNOLOGY

7. Restricting access to systems and data

- Physical access to computer networks, equipment, storage media and program documentation is restricted to authorised individuals.
- Logical access to computer systems, programs, master data, transaction data and parameters, including access by administrators to applications, databases, systems and networks, is restricted to authorised individuals via information security tools and techniques.
- Segregation of duties is defined, implemented and enforced by logical security controls in accordance with job roles.

8. Providing integrity and resilience to the information processing environment, commensurate with the value of the information held, information processing performed and external threats

- IT processing is authorised and scheduled appropriately and exceptions are identified and resolved in a timely manner.
- Data transmissions between the service organisation and its counter parties are complete, accurate, timely and secure.
- Appropriate measures are implemented to counter the threat from malicious electronic attack (for example firewalls and anti-virus software).
- The physical IT equipment is maintained in a controlled environment.

9. Maintaining and developing systems hardware and software

- Development and implementation of new systems, applications and software, and changes to existing systems, applications and software, are authorised, tested, approved and implemented.
- Data migration or modification is authorised, tested and, once performed, reconciled back to the source data.

10. Recovering from processing interruptions

- Data and systems are backed up regularly, retained offsite and regularly tested for recoverability.
- IT hardware and software issues are monitored and resolved in a timely manner.
- Business and information systems recovery plans are documented, approved, tested and maintained.

11. Monitoring compliance

- Outsourced activities are properly managed and monitored.

DATA PROTECTION / GDPR

12. Data Security

- Processing, storing and transmission of personal data is defined, implemented and enforced by security controls in accordance with job roles.

CONTROL TESTING

The control objectives have been tested during 2020/21 via the following methods.

CONTROL TESTING

OVERVIEW OF INTERNAL AUDIT ACTIVITY 2020/21

The internal audit activity to assess the control objectives for the financial year ended 31 March 2021 in regard to pension administration processes was undertaken by Deloitte.

OVERVIEW OF INTERNAL AUDIT ACTIVITY 2020/21

Deloitte were engaged to focus on assessing the design adequacy, implementation and operating effectiveness of key controls mitigating certain risks within the operational pension administration business.

The focus of the Audits of operational pension administration in FY20/21 have been around the calculations and payments of benefits to members, in particular, Transfer Values, Retirement and Death Benefits, the quality of the data received from Employers and recorded onto the Member records and the quality assurance of the processes.

Audits Conducted by Deloitte:

Control Objective 2 – Authorising and Processing Transactions		
Audit	**Controls**	**Exceptions (if any)**
Benefit Administration	Benefits payable and transfer values are calculated in accordance with scheme rules and relevant legislation and are paid on a timely basis	No Exceptions

Control Objective 3 – Maintaining Financial and Other Records		
Audit	**Controls**	**Exceptions (if any)**
Data Quality	Member records consist of up-to-date and accurate information and are updated and reconciled regularly. Contributions and benefit payments are completely and accurately recorded in the proper period. Investment transactions, balances and related income are completely and accurately recorded in the proper period	No Exceptions

Control Objective 2 – Authorising and Processing Transactions **Control Objective 5** – Monitoring Compliance		
Audit	**Controls**	**Exceptions (if any)**
Benefit Administration – Quality Assurance and on hold process	Services provided to pension schemes are in line with service level agreements. Transaction errors are rectified promptly and clients treated fairly.	Improvements were identified in the checking process which LPPA were already aware of and plans had been put in place to change the process accordingly.

OVERVIEW OF LPPA RISK & COMPLIANCE ACTIVITY 2020/21

This section contains details of the quality assurance and compliance monitoring activity for the financial year ended 31 March 2021 in regard to pension administration processes.

OVERVIEW OF LPPA RISK & COMPLIANCE ACTIVITY 2020/21

Reviews Conducted by LPPA's Quality Assurance & Compliance Monitoring Team:

For the FY20/21 LPPA's Quality Assurance & Compliance Monitoring Team have performed 3 quality assurance reviews on a monthly basis and 14 compliance monitoring reviews.

The remit of the Quality Assurance & Compliance Monitoring team is to ensure that LPPA administers pensions on behalf of it's Clients to the highest standards and in compliance with all rules and regulations that apply to a pension administration business, which includes the pensions legislation, the Pensions Regulator's Code of Practice 14 and Data Security to name but a few. The assessment of this tests the processes and procedures to ensure the appropriate controls are in place to mitigate risks to both LPPA and to the Client, as well as ensuring the LPPA values are being met which together drive a good customer experience.

The definition of Quality Assurance and Compliance Monitoring is:

Quality Assurance	Compliance Monitoring
Purpose: To drive business/process improvements **Objective:** An internal Management Tool	
Quality Assurance provides an early warning of any procedural/ skills/training gaps	Compliance Monitoring focuses on a process or business area to identify any efficiencies or drive continuous improvement

Quality Assurance

Control Objective 3 – Maintaining Financial and Other Records **Control Objective 5** – Monitoring Compliance **Control Objective 12** – Data Security		
Review	**Controls**	**Exceptions (if any)**
Helpdesk Calls Helpdesk Emails Check The Checker	Member records consist of up-to-date and accurate information and are updated and reconciled regularly. Contributions and benefit payments are completely and accurately recorded in the proper period. Investment transactions, balances and related income are completely and accurately recorded in the proper period. Services provided to pension schemes are in line with service level agreements. Transaction errors are rectified promptly and clients treated fairly. Processing, storing and transmission of personal data is defined, implemented and enforced by security controls in accordance with job roles.	Process improvements and knowledge gaps identified which are being addressed through the introduction of monthly team training sessions

Compliance Monitoring

Control Objective 2 – Authorising and Processing Transactions • **Control Objective 3** – Maintaining Financial and Other Records
Control Objective 4 – Safeguarding Assets • **Control Objective 5** – Monitoring Compliance
Control Objective 7 – Restricting Access to Systems and Data
Control Objective 8 – Providing integrity and resilience to the information processing environment, commensurate with the value of the information held, information processing performed and external threat
Control Objective 12 – Data Security

Review	Controls	Exceptions (if any)
Payroll Process	Benefits payable and transfer values are paid on a timely basis. Member records consist of up-to-date and accurate information and are updated and reconciled regularly. Benefit payments are completely and accurately recorded in the proper period. Funds are safeguarded and payments are suitably authorised and controlled. Services provided to pension schemes are in line with service level agreements. Transaction errors are rectified promptly and clients treated fairly. Physical access to computer networks, equipment, storage media and program documentation is restricted to authorised individuals. Segregation of incompatible duties is defined, implemented and enforced by logical security controls in accordance with job roles. Data transmissions between the service organisation and its counter parties are complete, accurate, timely and secure. Processing, storing and transmission of personal data is defined, implemented and enforced by security controls in accordance with job roles.	Standardisation of processes and enhancement to controls were identified and implemented. Control enhancements included the introduction of a second check stage prior to payment release and team training to remove a key person dependency.

OVERVIEW OF LPPA RISK & COMPLIANCE ACTIVITY 2020/21

Control Objective 2 – Authorising and Processing Transactions • **Control Objective 3** – Maintaining Financial and Other Records
Control Objective 4 – Safeguarding Assets • **Control Objective 5** – Monitoring Compliance
Control Objective 7 – Restricting Access to Systems and Data
Control Objective 8 – Providing integrity and resilience to the information processing environment, commensurate with the value of the information held, information processing performed and external threat
Control Objective 12 – Data Security

Review	Controls	Exceptions (if any)
Overpayments	Benefits payable and transfer values are calculated in accordance with scheme rules and relevant legislation and are paid on a timely basis. Member records consist of up-to-date and accurate information and are updated and reconciled regularly. Benefit payments are completely and accurately recorded in the proper period. Funds are safeguarded and payments are suitably authorised and controlled. Services provided to pension schemes are in line with service level agreements. Transaction errors are rectified promptly and clients treated fairly. Physical access to computer networks, equipment, storage media and program documentation is restricted to authorised individuals. Segregation of incompatible duties is defined, implemented and enforced by logical security controls in accordance with job roles. Data transmissions between the service organisation and its counter parties are complete, accurate, timely and secure. Processing, storing and transmission of personal data is defined, implemented and enforced by security controls in accordance with job roles.	Automation of case review reminders was recommended as an improvement to the process to ensure no cases are overlooked due to a requirement for manual intervention.

Control Objective 3 – Maintaining Financial and Other Records **Control Objective 5** – Monitoring Compliance **Control Objective 12** – Data Security		
Review	**Controls**	**Exceptions (if any)**
Helpdesk Call Handling	Member records consist of up-to-date and accurate information and are updated and reconciled regularly. Services provided to pension schemes are in line with service level agreements. Transaction errors are rectified promptly and clients treated fairly. Processing, storing and transmission of personal data is defined, implemented and enforced by security controls in accordance with job roles.	Call opening and closing scripts introduced to ensure consistency and improve data protection checks and validation that data held is up to date.
Helpdesk Email Enquiry Handling	Member records consist of up-to-date and accurate information and are updated and reconciled regularly. Services provided to pension schemes are in line with service level agreements. Transaction errors are rectified promptly and clients treated fairly. Processing, storing and transmission of personal data is defined, implemented and enforced by security controls in accordance with job roles.	Inconsistency of manner and format of responding to enquiries. A standardised email template was introduced.

Control Objective 3 – Maintaining Financial and Other Records **Control Objective 5** – Monitoring Compliance **Control Objective 12** – Data Security		
Review	**Controls**	**Exceptions (if any)**
Aggregation	Member records consist of up-to-date and accurate information and are updated and reconciled regularly. Services provided to pension schemes are in line with service level agreements. Transaction errors are rectified promptly and clients treated fairly. Processing, storing and transmission of personal data is defined, implemented and enforced by security controls in accordance with job roles.	Improvements were identified in the procedure notes and member correspondence. A record keeping issue was identified which if not addressed could have had an adverse impact on the McCloud remedy work.
Control Objective 5 – Monitoring Compliance **Control Objective 9** – Maintaining and developing systems hardware and software		
Review	**Controls**	**Exceptions (if any)**
Survey Responses	Clients are treated fairly. Development and implementation of new systems, applications and software, and changes to existing systems, applications and software, are authorised, tested, approved and implemented.	A marked reduction in survey responses was identified by the business. This Review revealed that the survey was not correctly configured and therefore members were not able to respond.

Control Objective 3 – Maintaining Financial and Other Records **Control Objective 5** – Monitoring Compliance **Control Objective 12** – Data Security		
Review	**Controls**	**Exceptions (if any)**
DPA Fails	Member records consist of up-to-date and accurate information and are updated and reconciled regularly. Services provided to pension schemes are in line with service level agreements. Transaction errors are rectified promptly and clients treated fairly. Processing, storing and transmission of personal data is defined, implemented and enforced by security controls in accordance with job roles.	The use of the disposition 'DPA Fails' was found to be incorrectly used and as a result has been removed.
Control Objective 3 – Maintaining Financial and Other Records **Control Objective 5** – Monitoring Compliance **Control Objective 12** – Data Security		
Complaint Handling	Member records consist of up-to-date and accurate information and are updated and reconciled regularly. Services provided to pension schemes are in line with service level agreements. Transaction errors are rectified promptly and clients treated fairly. Processing, storing and transmission of personal data is defined, implemented and enforced by security controls in accordance with job roles.	Complaint categorisation process implemented to speed up turn around times. Template final response letter developed.

Control Objective 3 – Maintaining Financial and Other Records • **Control Objective 5** – Monitoring Compliance **Control Objective 11** – Monitoring Compliance • **Control Objective 12** – Data Security		
Review	**Controls**	**Exceptions (if any)**
FCS Post	Member records consist of up-to-date and accurate information and are updated and reconciled regularly. Services provided to pension schemes are in line with service level agreements. Transaction errors are rectified promptly and clients treated fairly. Outsourced activities are properly managed and monitored. Processing, storing and transmission of personal data is defined, implemented and enforced by security controls in accordance with job roles.	No exceptions.
Control Objective 3 – Maintaining Financial and Other Records **Control Objective 5** – Monitoring Compliance **Control Objective 12** – Data Security		
Review	**Controls**	**Exceptions (if any)**
Helpdesk First Contact Resolution	Member records consist of up-to-date and accurate information and are updated and reconciled regularly. Services provided to pension schemes are in line with service level agreements. Transaction errors are rectified promptly and clients treated fairly. Processing, storing and transmission of personal data is defined, implemented and enforced by security controls in accordance with job roles.	The definition and process for first contact resolution was not fully documented.

Control Objective 2 – Authorising and Processing Transactions • **Control Objective 3** – Maintaining Financial and Other Records
Control Objective 4 – Safeguarding Assets • **Control Objective 5** – Monitoring Compliance
Control Objective 7 – Restricting Access to Systems and Data
Control Objective 8 – Providing integrity and resilience to the information processing environment, commensurate with the value of the information held, information processing performed and external threat
Control Objective 12 – Data Security

Review	Controls	Exceptions (if any)
Bereavements	Benefits payable and transfer values are calculated in accordance with scheme rules and relevant legislation and are paid on a timely basis. Member records consist of up-to-date and accurate information and are updated and reconciled regularly. Benefit payments are completely and accurately recorded in the proper period. Funds are safeguarded and payments are suitably authorised and controlled. Services provided to pension schemes are in line with service level agreements. Transaction errors are rectified promptly and clients treated fairly. Physical access to computer networks, equipment, storage media and program documentation is restricted to authorised individuals. Segregation of incompatible duties is defined, implemented and enforced by logical security controls in accordance with job roles. Data transmissions between the service organisation and its counterparties are complete, accurate, timely and secure. Processing, storing and transmission of personal data is defined, implemented and enforced by security controls in accordance with job roles.	Process review recommended to drive consistency across all clients. Process notes are old and should be reviewed and updated where appropriate. A review of the short term injury pension process for police & fire was instigated to remove inconsistencies.

Control Objective 3 – Maintaining Financial and Other Records • **Control Objective 5** – Monitoring Compliance **Control Objective 12** – Data Security		
Review	**Controls**	**Exceptions (if any)**
Helpdesk Complaint Handling	Member records consist of up-to-date and accurate information and are updated and reconciled regularly. Services provided to pension schemes are in line with service level agreements. Transaction errors are rectified promptly and clients treated fairly. Processing, storing and transmission of personal data is defined, implemented and enforced by security controls in accordance with job roles.	Member minor dissatisfaction is not being recorded and reported.

Control Objective 3 – Maintaining Financial and Other Records • **Control Objective 5** – Monitoring Compliance **Control Objective 6** – Reporting to Clients • **Control Objective 12** – Data Security		
Review	**Controls**	**Exceptions (if any)**
Accounting for Tax & Event Reporting	Member records consist of up-to-date and accurate information and are updated and reconciled regularly. Services provided to pension schemes are in line with service level agreements. Transaction errors are rectified promptly and clients treated fairly. Periodic reports to participants and scheme sponsors are accurate and complete and provided within required timescales. Regulatory reports are made if necessary. Processing, storing and transmission of personal data is defined, implemented and enforced by security controls in accordance with job roles.	Procedure guides require updating. Consideration to be given to improving reporting format to flag duplicate/incorrect data. Inconsistencies identified within services provided to clients.

Control Objective 3 – Maintaining Financial and Other Records **Control Objective 5** – Monitoring Compliance **Control Objective 6** – Reporting to Clients **Control Objective 8** – Providing integrity and resilience to the information processing environment, commensurate with the value of the information held, information processing performed and external threat **Control Objective 12** – Data Security		
Review	**Controls**	**Exceptions (if any)**
Bulk Data	Member records consist of up-to-date and accurate information and are updated and reconciled regularly. Services provided to pension schemes are in line with service level agreements. Clients are treated fairly. Periodic reports to participants and scheme sponsors are accurate and complete and provided within required timescales. Data transmissions between the service organisation and its counterparties are complete, accurate, timely and secure. Processing, storing and transmission of personal data is defined, implemented and enforced by security controls in accordance with job roles.	Identified the need to consider automation to remove the risks with manual intervention and key person dependencies.

ACCREDITATIONS

ACCREDITATIONS

LPP
Local Pensions Partnership
Administration

LPPA will continue to maintain the following accreditations in support of its control assurance framework.

Title	Expiry
ISO 27001	LPPA re-certification due in September 2021
Cyber Essentials	Re-certification successful in July 2021

LPP

Local Pensions Partnership
Administration

lppapensions.co.uk

This Internal Control Assurance
Report will be issued annually
covering the previous financial year.

Document is Restricted

This page is intentionally left blank

LPPA's cyber security measures

LPPA understands the importance of keeping member data secure. To ensure that the data under our control is kept secure, we have implemented a number of controls and technologies. Whilst technology is important in cyber security, the investment in training of staff is also a key factor in our defence against malicious acts.

LPP group (including LPPA) is ISO 27001 accredited and has Cyber Essential accreditation. This accreditation shows that it has processes and procedures in place that keep information and systems secure, which is independently verified.

System Security

All of LPPA's systems are protected at the network perimeter by firewalls, with Palo Alto firewalls in place at the main data centre. The firewalls are automatically updated to protect against emerging threats. Firewalls have a "default deny" policy, with changes to rules completed after a change control process is followed, with a business need and security review carried out. External penetration tests are carried out by CREST accredited organisations to verify the perimeter protection.

Servers and end-user devices are patched regularly, with critical patches installed within 14 days of release. All devices are covered by antivirus, which is centrally managed and updates are automatically downloaded to devices.

To protect against the loss of data, system corruption or ransomware, LPPA backs up data daily to tape, with tapes collected daily and sent to a secure, environmentally controlled storage facility. Data is restored regularly to test the restoration process and the backup media.

User Accounts & Access control

All users have dedicated user accounts, which require complex passwords. Domain accounts are protected with two factor authentication. Administrative accounts are separate from day-to-day accounts, with elevated privileges restricted to users who need them.

Access to systems and information is based on user role, with users only having access to data that they need, changes to user rights need to be appropriately requested. Access reviews are carried out regularly.

All default passwords and configuration is removed from new devices.

Incident Response

Whenever there is a risk to LPPA systems or data an incident response is started. The Security Working Group (SWG) is made aware and a response is handled by an Incident Response Team. The team is made up of representatives of the senior leadership team, risk, IT, communications and any other team affected.

Risk assessments are carried out whenever there is a critical vulnerability released, with both internal systems and suppliers monitored for their exposure and remediation.

External Services

Whenever an external software supplier is engaged, a risk assessment is completed, ensuring that the supplier has adequate levels of protection, security systems, encryption, processes and data is held within the UK where possible.

End Users and Home Working

With the move to home working, LPPA have had to implement changes to enable this. All users are provided with a company laptop, which is the only method they use to access systems. The laptops are protected with antivirus, web filtering, email filtering and archiving and are locked down to prevent unauthorised applications running. All company devices restrict the use of external devices to prevent homeworkers from connecting to personal printers etc.
All data on end user devices are encrypted using BitLocker, with users having to enter a code before the device boots.

Access to the LPPA network is via secure VPN using active directory credentials. The VPN client is updated regularly.

Improvements

Protection of data and systems is an ever-evolving area, with LPPA investing in improvements. LPPA is planning to implement a Security Operations Centre service in the next financial year, to improve its security profile.

The current DR process is being reviewed, moving to an online backup capability, whilst ensuring that backups will not be vulnerable to ransomware attacks.