

Assurance Report on Internal Controls

**XPS Administration Limited
AAF 01/20 and ISAE 3402
for the period 1 January to 31 December 2021**

Contents

Executive Summary	1
XPS Working Model	3
Corporate Philosophy	4
Statement by Service Auditor	6
Management Statement	7
Structure of the XPS Pensions Group	9
XPS Administration Business Structure	10
XPS Administration Governance	12
Control Environment	16
Report Statistics	26
Exceptions and Management Responses	27
Service Auditor Report	30
Summary of Control Objectives	33
Control Procedures and Service Auditor Tests	37
Appendices	142

Executive Summary

This report has been produced in accordance with the principles established in “Assurance Reports on Internal Controls of service organisations made available to third parties” issued as an AAF 01/20 by the Institute of Chartered Accountants in England and Wales (AAF 01/20) and the International Standard on Assurance Reporting 3402 (ISAE 3402) issued by the International Auditing and Assurance Standards Board (IAASB). XPS Pensions Group has adopted dual reporting under both AAF 01/20 and ISAE 3402.

This assurance report describes the control environment within which the business operated from 1 January to 31 December 2021 and is the first year of working with RSM UK Risk Assurance Services LLP (RSM) who we have commissioned to work with us on the new AAF 01/20 framework.

XPS Pensions Group is a UK specialist in pensions actuarial, consulting and administration.

XPS Administration Limited employs 800 staff in 14 offices across the UK providing services to 597 trust-based schemes covering over 949,000 members. It has become one of the leading providers of high-quality pensions administration services in the marketplace.

For the purposes of this report our Portsmouth Office, which came on-line in June 2021, was excluded from the audit, and will be included in the scope of the next scheduled report.

XPS Administration provides client and member focused solutions for occupational pension schemes. Administration is our core business and we put the member first by focusing on accuracy and the member experience. The high quality, robustness and consistency of our administration services is widely recognised in the market, and we have been ranked first five times in Professional Pensions’ survey of Third Party Administrators.

We continuously strive to find ways of improving the level of service delivered to our clients. Our strategy has been to focus on ensuring the delivery of high quality administration services, combined with commercial proposition that represents value for money. Pensions Administration has become an increasingly complex occupation and whilst we have invested significantly in our technology and IT infrastructure, it is our belief that it is the quality of interactions with pension scheme members which represents our key differentiator.

In support of our requirement to manage a quality-controlled administration business, we operate within a robust governance structure which ensures the clear flow of information and the decision making process. This enables us to react swiftly to regulatory change and stay at the forefront of developments in the industry.

Response to Qualified Opinion from 2020 AAF report

Our last published AAF 01/06 report dated July 2021 had 3 qualifications which related to controls 7.1, 7.2 and 7.3.

We recognised that you, our clients, needed to see improvements in these areas and therefore to address these qualifications, we engaged a working party comprising of Senior Management and IT, to investigate the issues identified. We subsequently reviewed and updated our processes in these areas to ensure that the controls operate in a robust and effective manner. We believe that the findings in this report reflect the improvements we have made in the areas of previous weakness.


We continue to work on strengthening our controls, and have made the following changes since the issue of our 2020 AAF01/06 report:

- › Physical access controls have been strengthened to include an additional weekly leaver check to ensure access passes are revoked in a timely manner when a member of staff leaves XPS.
- › We have introduced a single electronic leavers form removing the need for managers to send separate forms to individual departments and have added the ability to add forward leaving dates to the systems to ensure that access is automatically revoked on the day the member of staff leaves.

- › We have strengthened our process around temporary and contract staff ensuring that an end date is entered at account set up stage, automatically terminating the account. Any extension to the contract requires the manager to log a ticket for the date to be amended providing full visibility of changes to the account.
- › In line with our Qualification in section 7.3 of our 2020 AAF01/06 report, we have reviewed whether it would be practical to restrict access to test environments in our client applications. We have decided that as the staff members only see the data in the test environment that they would see in the live environment there is no benefit to making this change. Therefore we have chosen to accept this risk within our controls and will not be making any changes to the way access in this area is granted.

We believe that whilst these changes were not implemented until later in 2021, the findings from this AAF 01/20 audit show how committed we have been in rectifying the control weaknesses previously identified.

Our IT Infrastructure function has undergone changes following the appointment of a Chief Information Officer during the first half of 2021. We released a new IT helpdesk system, with our 1st Line support moving in-house, which has meant that for the first time since 2018, we have a fully in-house IT team. Our Application Support Team was moved from the administration business into the IT function providing a simpler, more streamlined experience for the end users of the service.



David Watkins
Managing Director
XPS Administration

XPS Working Model

March 2020 saw the shut down of the UK economy as Covid-19 took hold. Office workers were told to work from home with only key workers allowed to go about their normal daily working routine.

Being an office based operation at XPS, and in line with Government guidance, we worked swiftly to ensure that all of our staff were provided with the equipment and updated policies they needed to work from home ensuring that you, our clients and your pension scheme members continued to receive the service you expect of us.

As the weeks passed by we continued to monitor the guidance from the respective UK nations, sharing the information with staff to make sure they fully understood what was expected of them as a fast evolving situation continued to change and, as restrictions lifted, some staff gradually started to return to our offices whilst others chose to stay at home and work. During this time, it became clear that homeworking worked well in many areas of our business and it was with this in mind we elected to review our existing working model.

In February 2021 we consulted with staff through workshop sessions with each part of the business, spoke to our Employee Engagement Group and our Diversity and Inclusion Group, and took soundings from other companies within the sector. Over 80% of our colleagues wanted more permanent “flexibility” as shown in our staff survey but this meant something different to each person. So we decided to give our colleagues a choice between Home, Flexible and Office workstyles. We ran a trial from April 2021 to December 2021. There were some points when we had to put the trial on hold due to the return of Covid restrictions but the feedback from colleagues has been positive.

We have re-emphasised during the trial the importance of the choice of location being about how you can best meet your work objectives and how you can contribute to the team dynamics rather than solely being driven by personal motivations. Teams have worked well together to agree on working patterns that work best for their teams and we are looking to roll the new working model out permanently in the coming months.

Corporate Philosophy



Mission and corporate values

XPS Pensions Group are a UK-focused specialist in pensions investment and administration, providing a range of services and solutions to over 1,500 pension scheme clients. We also operate a defined contribution Master Trust, the National Pension Trust, and provide administration to SSAS's and SIPP's.

- › Our 1500+ employees work from 17 offices in 15 locations around the UK.
- › We work with pension scheme trustees, sponsoring employers and pension scheme members, with schemes ranging in size from less than £20m in assets to multi-billion pound pension funds.
- › We charge fixed fees for ongoing administration and advisory services combined with time-based fees for consulting advice and one-off projects. We work with clients based on open-ended engagement letters. Many of the services we provide are essential, non-discretionary requirements for UK pension schemes, required on a repeating basis to a statutory timetable. As such, much of our revenue is independent of the economic cycle.
- › A high proportion of our revenues are recurring, and we have a loyal base of clients who have worked with us over many years.
- › As the only UK pensions specialist listed on the FTSE we have the flexibility to not only think differently but to act differently.
- › Our structure means that we make long term transparent investment decisions that are for the good of our clients and their pension scheme members.
- › Solely focused on the UK pensions market, we remain agile; able to react and innovate at pace with a perfect balance of scale and expertise. With no competing priorities or distractions, it's true to say that we are passionate about pensions. It's all we do, nothing else.
- › As the need to secure financial security in later life becomes increasingly important, XPS Pensions Group are changing the way that we think about pensions and the way that they are structured, managed, administered, and delivered. We will constantly challenge the pensions industry to improve.
- › Better schemes, information, technology, and decisions. Better service expectations and ultimately, better outcomes for trustees, businesses and members.
- › Our clients trust us because we always put them first. We are reliable, we get things done, we simplify the complexity of the UK pensions market and always do what we say we will.
- › We are committed to help increase understanding, share knowledge, reduce risk, protect members, build long lasting relationships, and reduce cost.

We believe there is a better way.



Use of technology

XPS Pensions Group is at the forefront of pensions administration in the development of both technology and process. Client and scheme members can access up to date information and functionality over the web using our software. We integrate technology with business process through Electronic Data Management (EDM) and workflow technology, delivering cost effective services to clients.



Quality and improvement

The continuous monitoring, review and improvement of processes is fundamental to XPS Pensions Group and the administration business and is carried out in a structured and controlled manner. Within the Pensions Administration area we have a governance structure made up from a number of committees representing all areas of the administration business, who are responsible for delivering and managing technical developments and training to our staff and top class administration to our clients.

XPS Administration is certified to ISO 27001:2013 across all of its offices with Bristol (Cote House), Leeds and Belfast recently attaining certification.



Our culture

Our corporate values are embedded in everything we do. They guide the decisions we make, big and small, on a daily basis. They are at the heart of our performance management and promotion process and optimise our sustainable operation. Our values and behaviour are aligned with the expectations of our people, clients and scheme members.

Our culture, driven by our values, has yielded benefits for our staff and clients alike. We firmly believe that our culture translates directly into how we perform as a business. We are employee centric, and actively work to build and maintain a culture that is diverse and inclusive. We were recognised for this in 2020 when we won the overall Gold Award at the UK Business Culture Awards. At the end of last year, we were 'highly commended' at the awards for 'leading with purpose'.



Statement by Service Auditor

The Service Auditor's Report, as set out on pages 30 to 32, has been prepared solely in accordance with terms of engagement agreed by the Senior Management of XPS Administration Limited ('the Senior Management') with RSM Risk Assurance Services LLP and for the confidential use of XPS Administration Limited ('the Service Organisation') and solely for the purpose reporting on the Control Activities in providing an independent conclusion on the Management Statement set out on pages 7 and 8 hereof. Our Report must not be relied upon by the Service Organisation for any other purpose whatsoever.

We have, exceptionally, agreed to permit the disclosure of the Service Auditor's Report, in full only, to current and prospective User Entities of the Service Organisation using the Service Organisation's services ('User Entities') and to the auditors of such User Entities, to enable User Entities and their auditors to verify that a report by Service Auditors has been commissioned by Senior Management of the Service Organisation and issued in connection with the control activities Control Activities of the Service Organisation without assuming or accepting any responsibility or liability to them on our part.

The Service Auditor's Report must not be relied upon by User Entities, their auditors or any other third party (together 'Third Parties') for any purpose whatsoever. RSM Risk Assurance Services LLP neither owes nor accepts any duty to Third Parties and shall not be liable for any loss, damage or expense of whatsoever nature which is caused by their reliance on our Report. Should any Third Party choose to rely on the Service Auditor's Report, they will do so at their own risk.

The Service Auditor's Report must not be recited or referred to in whole or in part in any other document and must not be made available, copied or recited to any Third Party without our express written permission.

Statement by the Senior Management of XPS Administration Limited – Type 2 Report

As Senior Management of XPS Administration Limited (‘the Service Organisation’) we are responsible for the identification of Control Objectives relating to the provision of pensions administration services and related information technology by the Service Organisation and the design, implementation and operation of the Service Organisation’s Control Activities to provide reasonable assurance that the Control Objectives are achieved.

In carrying out those responsibilities we have regard not only to the interests of our clients but also to those of the owners of the business and the general effectiveness and efficiency of the relevant operations.

The accompanying description has been prepared for clients, who have used the pensions administration and related information technology services, and their auditors who have a sufficient understanding to consider the description, along with other information including information about Control Activities operated by clients themselves.

We have evaluated the fairness of the description and the design suitability of the Service Organisation’s Control Activities in accordance with the Technical Release AAF 01/20 (‘AAF 01/20’), issued by the Institute of Chartered Accountants in England and Wales, and the Control Objectives for pensions administration activities and related information technology services set out in AAF 01/20 and the International Standard on Assurance Engagements 3402 (‘ISAE 3402’), issued by the International Auditing and Assurance Standards Board.

We confirm that:


- A. The accompanying description on pages 1 to 25 fairly presents the Service Organisation’s pensions administration and related information technology services throughout the period 1 January 2021 to 31 December 2021. In addition to the Control Objectives specified in AAF 01/20, the criteria used in making this statement were that the accompanying description:
- i. Presents how the services were designed and implemented, including: the types of services provided, and as appropriate, the nature of transactions processed; the procedures, both automated and manual, by which client transactions were initiated, recorded and processed; the accounting records and related data that were maintained, reported and corrected as necessary; the system which captured and addressed significant events and conditions, other than client transactions; and other aspects of our control environment, risk assessment process, monitoring and information and communication systems, that were relevant to our Control Activities; and
 - ii. Includes relevant details of changes to the Service Organisation’s system during the period; and
 - iii. Does not omit or distort information relevant to the scope of the services being described, while acknowledging that the description is prepared to meet the common needs of a broad range of clients and their auditors and may not, therefore, include every aspect of the services that each individual client may consider important in its own particular environment.

B. The Control Activities related to the Control Objectives stated in the accompanying Description were suitably designed and operated effectively throughout the period 1 January 2021 to 31 December 2021.

The criteria used in making this statement were that:

- i. The risks that threatened achievement of the Control Objectives stated in the Description were identified; and
- ii. The identified Control Activities would, if operated as described, provide reasonable assurance that those risks did not prevent the stated Control Objectives from being achieved; and
- iii. The Control Activities were consistently applied as designed.

For the purposes of this report the control environment, control objectives and control procedures are applied in a consistent manner in all significant respects across XPS Administration's pensions administration and related information technology activities excluding our Portsmouth office which came on-line in June 2021 and will be included in the scope of the next scheduled report.



David Watkins
Managing Director

4 May 2022

Signed on behalf of the XPS Administration Limited Board of Directors

Structure of the XPS Pensions Group

XPS Pensions Group is the largest pure pension consultancy and the only listed pension specialist in the UK market.

We work with the trustees and sponsoring employers of UK pension schemes to deliver better outcomes for our clients. Our teams of actuaries, pension's specialists, investment consultants and administrators are dedicated to delivering excellence in customer service, clear advice and improved use of technology to facilitate effective decision-making by our clients and their pension scheme members.

XPS Pensions Group continues to be widely recognised in the market for their high quality, robustness and consistency. Our results bear testament to the strength of our business. We provide essential services to clients whilst we had to adapt to the challenges presented by the pandemic, we responded well. Total revenue has grown, driven by organic growth in all three pensions divisions along with the full year effect of the acquisitions of Royal London Corporate Pensions Services and Trigon Pensions. XPS Administration now provides administration services to over 597 pension schemes with our client schemes ranging from 20 to 75,000 members, in total servicing over 949,000 members.

The XPS Pensions Group comprises 'sister' subsidiaries, as shown below, whose services complement and mutually benefit the rest of the Group.



XPS Pensions Group



XPS Pensions

Advice and support to pension scheme trustees and sponsoring employers across all areas of UK pension scheme management, including actuarial advice and long-term financial planning for schemes, through to member communications, advice on member option exercises and scheme benefit design.



XPS Administration

Services including pension administration, payroll services, pension scheme accounting, scam identification, de-risking projects and technical consultancy for a wide range of trust-based company pension schemes, including defined benefit (DB), defined contribution (DC), career average revalued earnings (CARE) and hybrid schemes.



XPS Investment

Clear, independent advice to pension scheme trustees to enable them to make the optimum investment decisions for their scheme's assets. Using financial modelling of different mixes of asset classes, we help clients to choose the right portfolio for their needs, to maximise returns and/or minimise their level of risk.

We also provide:

- › The National Pension Trust (NPT), a defined contribution master trust for employers offering full 'Freedom and Choice' capability;
- › SIPP and SSAS solutions to financial advisers under the XPS Self Invested Pensions brand; and
- › XPS Arena, a destination for learning, support and development for people in pensions.

XPS Administration Business Structure

XPS Administration provides client focused administration solutions for occupational pension schemes. Our administration business provides a full range of pension administration services from 14* offices in 13 locations around the UK within a structured quality controlled environment.

XPS Administration Executive

David Watkins, our Managing Director, is supported by a team of Client Managers and Regional Operational Managers who are responsible for ensuring the smooth running of client services within the 14* XPS Administration Offices.



David Watkins
Managing Director



Gary Davies
Operations Director



James Peel
Client Services Director

Regional Operations Managers



Melanie Collins
Belfast
Reading
Wokingham
*Portsmouth**



Leighton Fisher
Edinburgh
Middlesbrough
Newcastle
Perth



Mary McLeod
Birmingham
Bristol
Leeds
Bristol Cote House
Chelmsford
London

*Portsmouth office out of scope for this audit.

Individual offices are overseen by Operations Managers. Administration Team Managers and their deputies are responsible for the ongoing delivery of client work and report to Operations Managers in relation to ongoing performance.

Our teams of pension administration staff provide services to a wide range of trust based pension schemes including: defined benefit, defined contribution, career average revalued earnings (CARE), hybrid and master trust schemes.

We seek to provide the highest levels of quality, and continuously strive to find ways of improving the level of service delivered to our clients and have been ranked first in Professional Pensions' survey of Third Party Administrators five times.

We use an individual scheme-based approach to administration, with one client team responsible for all aspects of our administration service. This ensures we focus on the needs of our clients and their scheme members, and that the quality controls we apply remain relevant and robust.

In support of our requirement to manage a quality controlled administration business we operate within a governance structure which ensures the clear flow of information decision making processes. This enables us to react swiftly to regulatory change and stay at the forefront of developments in the industry.

For the purposes of this report the control environment, control objectives and control procedures are applied in a consistent manner in all significant respects across XPS Administration offices excluding our Portsmouth office which came on-line in June 2021 and will be included in the scope of the next scheduled report.

PROFESSIONAL PENSIONS UK PENSIONS AWARDS 2021

HIGHLY COMMENDED

**Third-Party Administrator
of the Year**

XPS Pensions Group

PROFESSIONAL PENSIONS UK PENSIONS AWARDS 2020

WINNER

**Third-Party Administrator
of the Year**

XPS Pensions Group

XPS Administration Governance

Oversight & governance

XPS Group Business Review Meeting

- › To replace XPS Administration Executive Board
- › Oversight
- › Business governance
- › Strategic review / direction
- › Business development / investment decisions

Chaired by: Snehal Shah
Meets: Monthly

Risk Management Committee (RMC)

- › Oversees risk management framework, including strategic risk
- › Sets audit framework, both internal and external audits
- › Oversees legal & regulatory framework
- › Monitors compliance with legislation, regulation & internal policies
- › Works with AOC and Admin ExCo to ensure risks / issues raised & addressed

Chaired by: Snehal Shah
Meets: Every 2 months

Information Security Steering and Environmental Committee (ISESC)

- › Support the overall Information Security Management System (ISMS) in accordance with ISO27001, including the maintenance of all certifications.
- › Provide assurance and accountability to the Risk Management Committee for the management of ALL Information Security Risks across the Group in accordance to our Risk Management Policy and Information Security Policy Suite.
- › Provide Information Security Governance for the XPS Group, ensuring the successful delivery of the annual Information Security training and awareness programme.

Chaired by: Adrian Davison
Meets: Every 2 months

IT Security Governance Group

- › Agrees and reviews Information Security Programme
- › Develops and monitors key capabilities

Chaired by: Jon Marchant
Meets: Monthly

Core business committees

XPS Administration Executive Committee (Admin ExCo)

- › Sets business direction
- › Key decision making
- › Delivery of strategy, sets & monitors budgets & KPIs
- › Approvals – resourcing decisions, all budget spending, changes to T&Cs
- › Enforces continued compliance with legislation & regulations
- › Agrees policy & considers response to risk & compliance issues

Chaired by: David Watkins
Meets: monthly

Administration Operations Committee (AOC)

- › Responsible for the delivery of high quality services
- › Constant oversight / intervention in relation to all aspects of delivery to clients
- › Monitors resourcing levels and capacity planning
- › Escalation of key business risks / issues to Admin ExCo & RMC
- › Oversight of staff development – via Training & Development Committee
- › Oversight of operational efficiency initiatives
- › Monitors the delivery of agreed SLAs & agrees intervention actions
- › Oversees continued compliance with legislation & regulation

Chaired by: Gary Davies
Meets: Monthly

Administration Leadership Group (Leadership Group)

- › Reviews YTD financial performance & forecasts
- › Reviews and agrees Admin strategy
- › Plans for the future

Chaired by: David Watkins
Meets: at least quarterly

Steering committees

Operations Manager Group

- › Information exchange
- › Delegate decision making
- › Consistent approach to delivery
- › Idea sharing & debate
- › Continuous improvement initiatives
- › HR issues
- › IT issues

Chaired by: Rotation
Meets: Monthly

Training & Development Steering Group

- › Review training requests received and allocate budget
- › Consider additional training needs
- › Work with external training providers to develop appropriate courses where these don't currently exist
- › Co-ordinate professional qualification applications and exam entries
- › Continuous development of Actus and ensuring it is used by everyone
- › Interaction with T&D at Group level

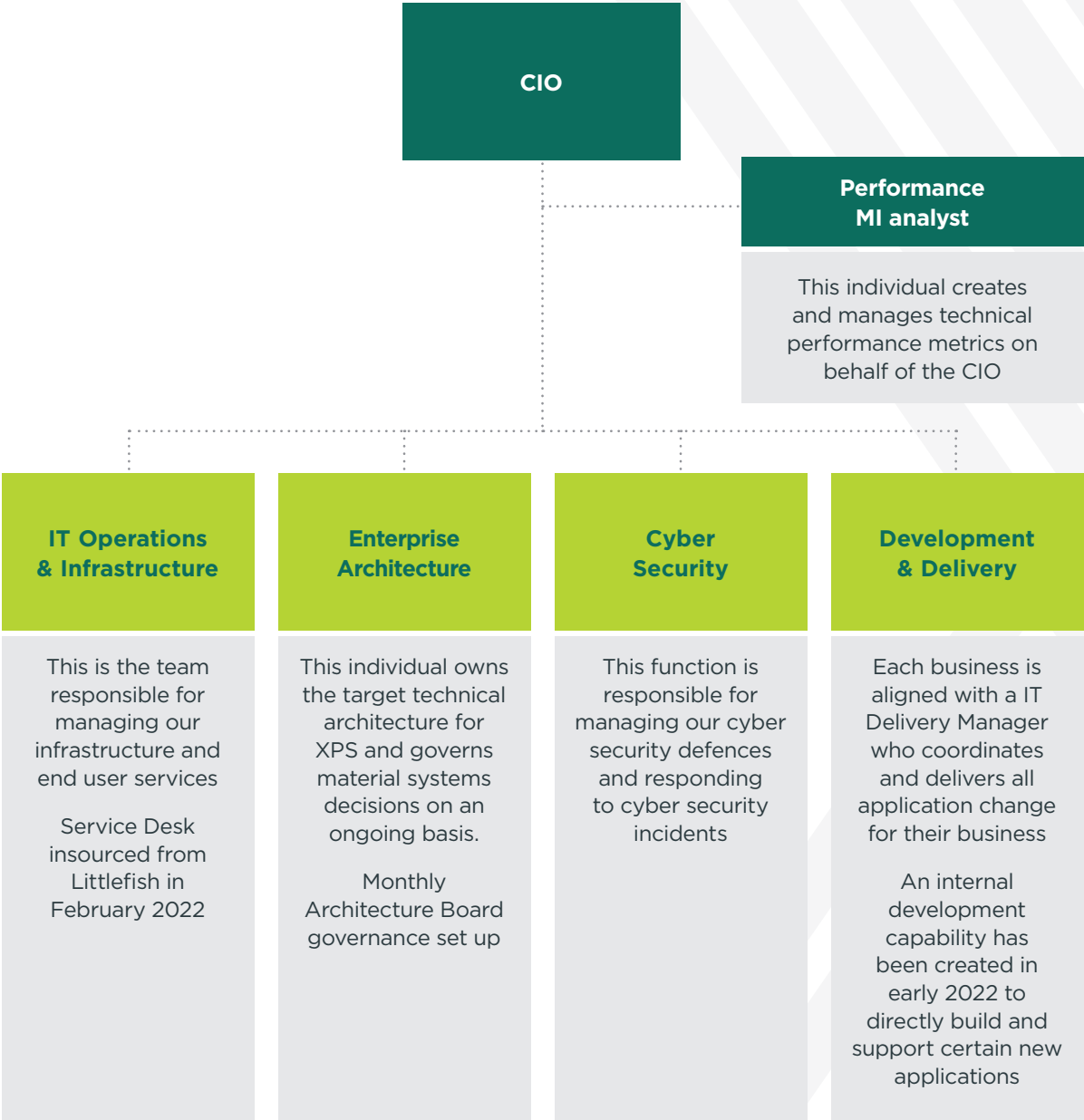
Chaired by: Mary McLeod
Meets: at least quarterly

CMT/Business Development Steering Group

- › Oversight of the commercial relationships for Administration only clients
- › Review of the pipeline for new opportunities
- › Manage the CMT framework, ensuring it is applied for Full Service contracts
- › Oversight of relationships and communications with Procurement Consultants

Chaired by: James Peel
Meets: approx every 6 weeks

High Level IT Structure Chart



Control Environment

The Directors of XPS Pensions Group are committed to deploying a strong control environment throughout the company. This control environment for pension administration services is achieved through the following measures. These measures were the same during the period of 1 January to 31 December 2021 unless otherwise stated.

Risk management

XPS Administration operates within the formal risk management framework provided by the XPS Group. This framework has been agreed by XPS Group Board and provides all businesses within the Group with policies and guidance on how risks should be identified and the controls required to manage these risks within agreed appetites. This framework uses a “three lines of defence” model with the Administration business supported by a central Risk function who provide oversight and co-ordinated reporting to the Audit and Risk Committee which is a subsidiary of the Group Board. This Risk function also co-ordinate assurance frameworks across the Group and the work of the independent internal audit function.

The Administration business uses this framework and co-ordinates its risk management activities via its Admin ExCo. This committee meets on a regular basis and is responsible for ensuring that business level risks are managed effectively and that Group mandated policies and controls are in place and operating effectively. Admin ExCo is responsible for the following areas relating to administration:

- › Risk management and reporting.
- › Internal and external audits.
- › Internal control framework.
- › Fraud prevention.
- › Business continuity.
- › Complaints and errors.
- › Supplier management.
- › Data Protection and Information Security.
- › Contractual agreements.

XPS Administration maintains Operational and Business Risk Registers which are reviewed on a regular basis by the Admin ExCo. We work with clients to identify and understand the key risks which apply to their schemes and how they interact with our own Risk Registers so that we can identify and implement measures to effectively mitigate these risks.

Business continuity

Business Continuity Management (BCM) is fundamental to the risk management strategy of XPS Pensions Group. The XPS Group Board recognises that the risk of serious unplanned interruptions needs to be addressed, to ensure that we can comply with our regulatory requirements and maintain the level of services our clients require. BCM is managed centrally, with the Group Board, supported by the Audit and Risk Committee and the Risk Management Committee, responsible for ensuring that an effective business continuity framework is in place and maintained.

Our BCM programme is aligned to ISO22301 and the Business Continuity Institute's Good Practice Guidelines. The primary objective of our programme is to ensure that critical business functions and processes are prioritised and recovered within predetermined timeframes in the event of a major operational disruption. This helps to ensure that in the event of a disaster the Group will have the capability to restore all critical client facing operations within 4 hours, and otherwise within 24 hours. To do this, we have introduced resilience strategies, recovery objectives, business recovery plans and incident management tools.

IT Disaster Recovery is the responsibility of the IT Director. XPS's IT infrastructure includes hosted tier 3 data centres (DC's) across which key systems are replicated providing day-to-day operational resilience and defence against a single DC failure as systems can be brought up at the alternate. When an incident impacts the Group, the Group Incident Management Team is invoked to provide strategic direction to Tactical Recovery Team(s) within the affected businesses in implementing their Business Recovery Plans. This approach ensures strategic, prioritised recovery of critical processes, clear communication throughout the business and to our clients and stakeholders, and consolidation of the resources required for recovery.

The centralised BCM framework ensures that plans are updated and tested annually. If no change prompts such an update then the annual review, test, update and sign-off process ensures the currency of those plans. Business Recovery Plans are tested twice annually; once focusing on the IT Disaster Recovery elements and once focussing on business operations, e.g. denial of access to an office. This approach ensures that the relevance of the data being maintained in the plans is always tested in relation to a viable IT environment. All-staff rapid notification tests are also carried out at least annually.

If any office is inaccessible for more than half a day, our displacement strategy ensures that critical functions can continue to be supported from predesignated alternative sites, i.e. an alternative XPS office or via home working.

The Group's IT Disaster Recovery capability is also tested throughout the year to ensure that the plans and procedures remain current and provide the correct capabilities.

During 2021 we also carried out planned tests of our IT Disaster Recovery capability, successfully restoring the critical systems in scope. The Group also successfully carried out several live rapid notifications to staff providing updates in relation to the ongoing Business continuity incident in relation to Covid-19.

In addition to the above, Business Continuity capabilities are included in our third party selection and ongoing monitoring processes. This will include identifying alternative suppliers for critical services to ensure that supply chain issues do not impact our ability to provide services to our clients.

Data protection and GDPR

XPS Pensions Group takes data protection very seriously, and all staff are required to follow the principles contained within GDPR and Data Protection Act 2018 legislation.

To assist in maintaining compliance with data protection principles, XPS has appointed a Data Protection Manager who is responsible for data protection matters within the Group and reports to the XPS Executive Board.

We have carried out the following steps which are reviewed and updated on an annual basis:

- › Mapping all data processed by XPS Administration – including data maps and a data inventory. This is reviewed annually to ensure that it remains current.
- › Updating policies and processes to ensure compliance with GDPR, for example: breach management plan, handling subject access requests, data retention policies etc.
- › Establishing a DPIA framework and carrying out DPIAs where required.
- › Gathering data regarding our third party sub-processors to confirm that their data protection and information security controls are compliant with GDPR.
- › Reviewing and updating client and third party contractual Data Protection Agreements.
- › Reviewing and updating our own privacy notices and member communication templates.
- › Organising staff awareness training – mandatory training is provided to all staff on information security and data protection on joining XPS and at least annually thereafter.

Data encryption

Client data is only processed on XPS managed devices. Data is stored centrally in DFS not locally on the device and local storage is redirected to DFS. All remote access to data is via Virtual Private Network (VPN). High risk Servers are configured with OS level encryption using BitLocker with AES 256-Bit encryption.

Transferring data

Personal data is transferred in line with our Information Classification & Handling and Data Transfer policies, which stipulates who can authorise the sharing of data and how this can then be done securely.

All electronic external data transfers involving client personal data or business confidential information are secured with Transport Layer Security (TLS) using AES 256-bit encryption. All electronic external data transfers involving client personal data or business confidential information are secured. Our secure upload website is used to securely transfer bulk data to any third party.

When transferring confidential information, we recommend that clients use our secure upload site or other such secure channels.

All client data held will remain in the UK/EEA. We only transfer data outside of the UK/EEA on the written instructions of the trustees, client, Data Controller or Data Subject. Any authorised transfer will require the data to be transferred via secure channels. Where we use third party suppliers to support our administration service, any data they process on our behalf is stored in the UK/EEA.

Retention and destruction of data

In line with the principles of GDPR and the Data Protection Act 2018, we ensure that we store data for only as long as is required. Data retention periods are agreed as part of our contractual negotiations, and we retain data in line with contractual agreements with our clients, and as outlined in our Privacy Policy.

Media, system and paper disposal is conducted via approved third party suppliers and audited as part of this AAF report.

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.

XPS Pensions Group adopts a proactive approach to cyber / information security. The Chief Information Officer (CIO) is responsible for managing IT / information security and has appointed an Information Security Manager to assist with the management of information security risks across the Group, along with a team of Information Security analysts. Our Data Protection Manager is responsible for monitoring data confidentiality and ensuring compliance.

The Information Security and Environmental Steering Committee (ISESC) 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 ISO27001 standards.

XPS Administration has certification to ISO27001, covering all its activities and offices. Our certification is audited twice yearly by our accredited assessors, LRQA. In June 2021 we also successfully obtained certification to Cyber Essentials Plus.

This is supported by a comprehensive suite of Information Security policies, 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 Group's systems and that they are forced to change their passwords at least every 60 days. We have introduced Multi-Factor Authentication (MFA) to access the XPS Network via VPN.

Our business continuity frameworks ensure that our service remains highly available. This ensures that multiple copies of data are available and resilience is in place should an incident impact one of our data centres.

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 the IT Operations Manager. 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.

Physical security

We recognise the importance of ensuring that our office locations remain secure and that we protect client data. We have strong physical security controls in place across our office locations which are audited as part of this controls report.

We use a contracted service provider (Backbone Connect) to provide WAN and Data Centre services. Backbone use Tier 3 colocation data centres

provided by Century link and Digital Reality to host our equipment which is in dedicated racks only accessible to us. They have a combination of the following physical security controls in place to protect the premises:

- › 24/7 guards
- › CCTV
- › Physical access controls (card readers – role specific)
- › Perimeter security
- › Restricted access points
- › Visitor registration procedures and visitors escorted on site.

Incident Management and breach reporting

We have documented standard procedures in place for dealing with suspected and actual cyber security events, incidents, breaches and cyber-attacks. These are tested regularly to confirm their effectiveness and updated at least annually.

Data Breaches are handled in line with our Data Breach Process & Investigation, which requires that a full report is provided to the data controller as soon as possible after we become aware of a data breach having occurred. All Cyber Security incidents are logged in a ticket management system and Governance Register and handled in line with our Incident Management and Breach Reporting policy.

Clients will be notified as soon as possible of any suspected or actual security event which may have compromised any of the client's confidential information.

In the event of confidential information being potentially compromised our procedures are designed to support us to effectively co-operate with clients in relation to investigation and remedial actions as may be required.

Internal audit

An Internal Audit function is in operation, using a co-sourcing agreement with PwC. It offers independent oversight of operational and risk management activities, with audit reports and relevant findings presented to the Audit and Risk Committee. The Internal Audit programme is supported by a number of regular assurance activities which are carried out by the internal Risk

and Compliance teams, which look at the design and effectiveness of internal controls for key processes. All audit findings are recorded on our Corrective Action Plan and tracked through to completion.

IT strategy

The effective use of IT is central to XPS Pensions Group's approach to pension administration. A Chief Information Officer (CIO) was appointed in May 2021 (an additional new role in the Group) who has taken on responsibility for ensuring that XPS Pensions Group has a robust technical strategy in place, sufficient to deliver a high-quality service to our clients and their members. Our aim is to be an industry leader in the use of technology.

A significant investment in technology and technical staff is being made to deliver on this aim with a particular focus on improving our processing efficiency, improving the quality of our overall service and in particular improving the digital experience of members. We run a 'best of breed' systems model in our business, choosing and integrating a number of best-in-class 3rd party systems with our internal systems and this allows us to adopt a continuous improvement approach to keep ourselves at the forefront of technological innovation within the pension administration industry.

Our third party system partners support our new centralised IT function in the management and maintenance of the Group's technical Infrastructure, including implementation of initiatives to strengthen the overall core technical infrastructure to support XPS's business functions, further enhance security and increase overall business flexibility and responsiveness.

Third party management

XPS operates a third-party management framework which ensures that all suppliers meet the necessary requirements to protect the information assets they may be given access to.

The Group has a formal selection process that ensures due diligence is carried out, which is proportionate to the risk of the potential failure/security exposure of the third party. We use a supplier management platform, Prevalent, to assist with managing our third party suppliers and to ensure that they comply with the standards required by XPS Pensions Group and their clients.

All third parties are reviewed prior to any access to information being granted and at regular intervals during life of the contract. The regularity of those reviews are determined using a risk based approach and all suppliers are allocated a tiering status with tier 1 being allocated to those who pose the highest level of risk to the Group or our clients and tier 3 with the lowest potential risk exposure. As part of our ongoing review process, copies of independent audit reports are obtained and reviewed on an annual basis for key suppliers to validate that their security controls continue to operate effectively. In addition to this, we also have in place regular monitoring of service delivery, general governance and financial status of all key suppliers we contract with.

Our framework ensures contracts include key risks relating to services provided and that risks identified during due diligence are managed and accepted prior to agreements being signed. Where there is a reliance on a single supplier, contingency plans are in place to protect against failure.

Training and development programme

XPS Pensions Group staff recruitment is conducted in accordance with clear formal policies and guidance on equal opportunities and diversity in the workplace. This applies whether candidates are applying through the administration apprenticeship arrangement introduced in 2021, or for non-apprentice roles.

We have a defined policy on staff development underpinned by competency based benchmarking through our Administration Role Framework system. In support of this structure XPS Pensions Group maintains a dedicated and properly resourced training function to support central training requirements. In addition, we have a specialist Administration Training and Development team to enhance the specialist training and development in this business area and support holistic development of staff.

All employees carry out annual training in relation to Awareness of Bribery and Corruption and Anti-Money Laundering and GDPR as a minimum and additional soft skills and technical skills aimed at specific roles and grades.

We have developed a bespoke training plan for our apprentices to develop their skills and help them to develop within their roles. In addition, all of our managers and deputy managers take part in our XPS Administration Management training program.

We recognise that the most important way to ensure that we protect client data is to ensure that our staff understand the importance of and how they can protect client data. All staff complete mandatory Information Security and Data Protection training as part of their initial induction into the company. This is endorsed by senior management and courses are reviewed on a regular basis by our Information Security Manager.

In addition to this, mandatory annual online refresher training is provided, along with ad-hoc awareness briefings throughout the year to address specific hot topics.

Pensions Administration staff are encouraged to obtain professional and vocational qualifications and are offered support in terms of a formal study package including study leave, the financing of study material and financial incentives for success as well as internal mentors.

We use the Actus performance management portal. This allows staff to own and control their own development through regular meetings with their manager and mentor. Staff set individual objectives and track their development as well as requesting training and recording the training they complete. The system also allows the collection of feedback from peers and a 360 feedback tool.

We hold an IIP Accreditation 'Silver Status' which was successfully renewed in September 2019 following an independent accreditation review.

Compliance

Our Administration Services Group (ASG) is a central team that assesses the impact of legislative change which may impact our clients and administration processes. Changes are communicated to staff via technical updates and face-to-face discussions. ASG maintains an intranet site accessible to all administrators providing a central reference point for technical materials, procedural guidance, standard letter templates and checklists.

XPS Administration are supported by Group Compliance, Risk and Group Legal where required.

Management information

Our corporate governance structure includes an Admin ExCo and an Administration Operations Committee (AOC), who meet monthly to analyse key management information.

A management information pack is distributed to the group for these meetings which has been designed to capture management information on all aspects of the administration business.

This information provides the Admin ExCo and AOC with the tools required to identify any risks or issues, with a view to agreeing rectification measures which in turn flow back to the administration teams.

Information and communication

Where our clients require it, we report our performance against agreed standards through an administration report which is prepared for each trustee meeting. The report includes details and commentary on various aspects of the running of their scheme.

The report has been designed to assist with the trustee governance requirements in accordance with current legislation and the Pension Regulator's guidance.

Fraud prevention

XPS Pensions Group risk assessment includes an internal assessment of fraud risk. XPS Pensions Group employs a variety of accounting and internal control systems that are designed to prevent and detect fraud and error.

Administration technology

We are constantly evaluating and reviewing our administration systems and infrastructure and have introduced a number of significant improvements over the past few years.



Penscope, our system of choice, was originally developed in-house and in 2009 we entered into an outsourcing contract with the pension software and transition management company, ITM. Accordingly, ITM now own the rights to PenScope and provide support and further development to us under contract.

We have made, and continue to make, a significant contribution in the development of the PenScope administration system, to ensure that it represents leading edge technology, and that it fully supports

our focus on quality, accuracy and efficiency.

The main features of PenScope are:

- › It is designed based on extensive experience of final salary, money purchase, hybrid, cash balance and CARE schemes.
- › It is a browser based application with a zero client install.
- › The application database is run on the industry standard MS SQL Server providing flexible access to the database content.
- › A .NET framework provides a centralised and well managed calculation engine coded in the widely used VB.NET programming language.
- › Web Services enabling integration routes for third party products and our own member web-access offering.



MyPension.com

We continue to roll out **MyPension.com** to a number of our clients providing them with the ability to offer online access for their members to the details we hold on our administration system (PenScope). Trustee access to scheme membership data is also supported via MyPension.com.

Some current features for defined benefit schemes include:

- › Access for active, deferred and pensioner members to personal details.
- › Members can view and amend contact and expression of wish details.
- › Members can post enquiries directly to their administration team with the enquiries falling directly into Alfresco our Business Process Management (BPM) system.
- › Where calculations are automated on PenScope members can perform online calculations and receive immediate online quotations.
- › Members can view their personal documents e.g. benefit statements, leaver statements and e-payslips.
- › Members can view scheme documents e.g. booklets and forms.

- › Client (pensions manager or trustee) access with ability to search and view member records.
- › Design (logos and colour scheme) can be tailored for a small additional cost to match clients' corporate branding.
- › Bulk upload and presentation of off-line member calculations.
- › Client specific DB Modellers such as Transfer Values.

In addition to the above, features for defined contribution schemes include:

- › Members can view their latest fund values.
- › Request changes to their fund choices and contribution rates.
- › Access a DC Modeller and run pension projections.
- › Multi-platform access including browsers, tablet and smart phone.

As well as providing access to member data mypension.com also has a pre authentication site that can be tailored to the client's needs. This area allows for richer member communication to a broader scheme membership by providing an area for the Trustees and the sponsoring business to present scheme specific information in a dynamic and engaging format.



Alfresco is our converged Electronic Content Management (ECM) and Business Process Management (BPM) system used to create efficient, connected processes that present member and scheme documents to our administration teams in a single browser interface.

By utilising its inbuilt functionality we are able to better manage and audit our administration processes as well as integrate with our administration and reporting systems.

Some of our current highlights include:

- › The integration of a Central Member Database (CMDDB). This is our master data source to client

data pulled from our various administration systems and is used to accurately tag content with the most current, relevant and accurate personal member data.

- › Dynamic in flow check-list guiding administrators through the process and ensuring benefits are accurate and compliant.
- › Integration with our reporting systems allowing us to report historical and current work item status and Service Level Agreement counters.
- › Cross platform workflows that allow for client work items to span administration functions.
- › Integration to supporting administration systems such as resourceLink (Payroll) and Compendia (Admin Platform) allowing automated data transfer of case work and common data sets.



Aquila Heywood

Altair is a powerful pensions administration and payroll platform provided by Aquila Heywood. It is a flexible browser-based system, providing efficient back office pensions administration and online portals for members and employers.

Our Altair deployment is used to administer Public Sector clients where it has a strong functional excellence.

System facilities include:

- › In built calculations producing either individual or bulk results – industry leading calculation engine for public sector pension administration.
- › Integrated electronic document management system – covering integration with MS Word and comprehensive image scanning/archiving tools.
- › Integrated workflow – user task lists, dashboards and SLAs.
- › Integrated Payroll – fully integrated with administration platform, web integration, reporting, HMRC compliant (RTI).
- › Member Self Service portals for scheme members to access their pension online including benefit projections.
- › Employer Self Service portal for scheme

employers to supply member employment changes.

- › In built reporting and data interfacing tools.



A browser based administration system used to administer NPT and former Xafinity Consulting Trust Based Clients.

The main features of the system are:

- › Readily deployable to support modern working practices.
- › Proven, fully scalable inbuilt workflow management system.
- › Integrated Electronic Document Management system providing on-demand access to member documentation.
- › Extensive suite of supported APIs enabling advanced member self-service functionality.
- › Advanced bulk processing via scheduled services.
- › Fully configurable, parameter driven calculations engine for the production of DB and DC calculations.



Profund Classic and **oPen2** are the administration systems used to administer our clients based in our Bristol Cote House office. The systems were inherited as part of the acquisition of Trigon Professional Services Limited in 2019 and work is already underway to migrate schemes off both these platforms and into our preferred administration platforms with payroll services having now been migrated to ResourceLink payroll.

Profund Classic – A proven industry standard pensions administration and payroll system suitable for all aspects of regular and bespoke administration tasks for Defined Benefit, Defined Contribution, Career Average and Hybrid schemes.

It offers:

- › Comprehensive record keeping.
- › Inbuilt comprehensive pension calculations.
- › Inbuilt reporting.
- › Integration with Microsoft products.
- › Compliant with relevant pensions regulations.
- › Fully integrated inbuilt work tracking flow.
- › Inbuilt pensioner payroll.
- › Fully integrated with electronic document management.

Profund oPen2 – A modern windows based scalable and configurable solution for Defined Contribution, Defined Benefit, Career Average and Hybrid pension schemes with fully integrated RTI compliant payroll.

It offers:

- › Comprehensive scalable record keeping.
- › Inbuilt comprehensive pension calculations.
- › Inbuilt Crystal reporting.
- › Full integration with electronic document management.
- › Full integration with workflow management.
- › Online member access.
- › Inbuilt pensioner payroll.
- › Straight Through Processing and Integration with Altus.

Profund Aviary is an innovative accounting solution created specifically for occupational pension schemes and third-party administrators. The system is designed to turn data into management intelligence with the minimum of time and effort through the use of automation and the 'Key Once' philosophy. It was purposely designed to meet the unique demands created by members and investments, rather than suppliers and income as in a conventional ledger. Additionally the integrated report and accounts production tool, Aviary Draft Accounts Reporting (ADAR), provides simplified production of compliant Pension Scheme Reports and Accounts.

Profund Aviary is a best of breed accounting application and is used by more than 1,500 schemes, ranging in size and complexity, to manage their pension scheme accounts.

CASHFAC

TECHNOLOGIES

CashFac is virtual banking software introduced to support our accounting and treasury services allowing us to adopt full electronic banking and payment functionality. CashFac links to our banking partners to deliver up to date transactional information by 8am each day. Thus we have removed the risks associated with paper based cashing processes and made significant efficiency gains.

CashFac enables the following:

- › Automated payments including BACS, CHAPS and SWIFT.
- › Consistent control of all cash management regardless of bank.
- › Automatic daily bank account reconciliation
- › Secure, distributed and tailored user access to scheme bank accounts and cash analysis across multiple locations.
- › Simultaneous payment and cash analysis in multiple currencies. An online audit trail for all transactions and events.
- › Tailored reporting based on business criteria.
- › Automatic Transaction Matching and Allocation suggests matches for receipts that lack reference data for automated matching.
- › Integration with Alfresco to allow one click retrieval of supporting transaction documents

Over 90% of the clients to whom we provide client banking services have now moved over to CashFac, enabling greater control and security on the service we provide.

zellis

Client payrolls are managed by our central specialist pension payroll team based in Newcastle. The **Zellis ResourceLink** platform is a proven and comprehensive payroll system that has been

engineered to provide key users with all the flexibility and functionality that they require to enable them to carry out their day to day activities effectively and efficiently. It also enables those users to utilise powerful analytical and reporting tools to allow them to analyse and distribute information in real time. ResourceLink is scalable so as to accommodate many thousands of employees/ pensioners. Robust security and comprehensive audit features also ensure the integrity of the solution – all historical information is available on-line at all times.

Currently we have integration in place that:

- › Integrates payroll records added and amended within our CMDB.
- › Automated new starter process via Alfresco workflow, securely adding new pensioner records to payroll from our Administration platforms – removing any need for double data entry.

Altus Business Systems

We introduced the **Altus Investment Gateway** (AIG) into our technology framework to enable 'Straight Through Processing' (STP) for both Defined Benefit (DB) and Defined Contribution (DC) investments wherever possible. STP is the end to end management of investment transactions, utilising technology and automated system controls, to minimise manual intervention and therefore to reduce risks.

With our Administration platforms and AIG being fully integrated into them, we can load Client generated contribution files directly in to PenScope, where they are validated, approved, and investment instructions securely passed to the AIG. Once received by the AIG the deal is complete, confirmation and prices are passed into the gateway from the fund manager, and order messages to the fund managers (utilising the Via Nova standard). Confirmations, price & holdings along with transaction data and reports are passed directly back into PenScope where member records are updated and fund / unit reconciliation can be completed.

Future technology developments

We will not step away from our fundamental belief that quality administration requires quality people, and not simply investment in technology. That said we recognise the importance technology has to play in helping to provide efficient, accurate and high quality services.

This year:

- › We have recently completed the migration from the Alfresco Workdesk build and onto the latest Alfresco 6 iteration. During this migration we implemented a change to the way workflow was managed, allocated and presented to end users. This year we will be building on the foundations laid to extend workflow and provide even greater control and automation. To aid with this we have created a new user / working group of users and administration leaders to start laying down the requirements for this program of works.
- › Additionally, we will be moving the system out of our datacentre and into our Microsoft Azure tenancy. Here we will be taking advantage of some of the enterprise technologies at our disposal as well as the rapid provisioning of compute and storage Azure has to offer.
- › Following the successful proof of concept with AWS and Alfresco where we were able to demonstrate the integration of robotic scanning, data retrieval and data ingestion from historical image files, we are now speaking to several clients to understand the practical application of this technology service into our service offering.
- › The use of RPA (Robotic Process Automation) software is already embedded into our IT estate and we are extending the use of these services to enhance the processing of document assembly and distribution.

Client control considerations

The control procedures relating to pension administration activities cover only a portion of the overall internal control structure of each client account (together termed 'User Entities'). Each client must evaluate the control procedures detailed below in conjunction with the controls in existence at their own organisation.

This section highlights those control responsibilities that we believe should be present for each client and has considered when developing the control procedures described herein.

The controls described below are intended to address only those controls surrounding the interface and communication between each client and XPS Administration Limited. Accordingly, this list does not purport to be, and is not, a complete listing of the controls which clients may need to have in place.

- › Instructions and information provided to XPS Administration Limited are in accordance with the provisions of the agreement governing the account or other applicable agreements between XPS Administration Limited and the client.
- › Timely written notification of changes to the client account objectives, guidelines or provisions of the governing agreement is made to XPS Administration Limited.
- › Timely review of reports provided by XPS Administration Limited is performed by the client and written notice is provided of discrepancies, if any, with the client's own records.
- › Timely review of invoices for fees and written notice of discrepancies, if any, with market values with appropriate client records.
- › Timely written notification of changes to individuals authorised to instruct XPS Administration Limited regarding activities on behalf of the client, is made to XPS Administration Limited.

Report Statistics

The AAF 01/20 and ISAE 3402 framework is flexible and subject to significant differences of interpretation. A firm's business objectives and its risk appetite will drive the nature, extent and depth of the internal control environment. The statistics here may assist in the understanding of the nature and extent of XPS Administration's internal controls but are not a reliable measure for comparison.

Risk area	Control objectives	Control count	Exception count
Accepting clients	3	10	0
Authorising and processing transactions	3	33	2
Maintaining financial and other records	5	19	1
Safeguarding assets	2	14	0
Managing and monitoring compliance and outsourcing	4	14	0
Reporting to clients	2	6	0
Information technology	17	84	2
TOTAL	36	180	5

Exceptions and Management Responses

2.3.6b Control

The payment output file is downloaded from the PAS by an Administrator for payment.

This then follows the standard payment process (see control 4.2.3d).

Note – Control in operation until June 2021.

Exception noted

For a sample of schemes and payments, due to the set up of the NatWest Banking system for payment, review by two Senior Administrators occurs after the payment is set up in the system for payment, therefore, an exception is noted.

The control cannot be evidenced as described due to the NatWest set up. It was noted that for the sample of payments reviewed, these matched payment processed.

Management response

The NatWest Banking Online system is a legacy system which was used in our Bristol Cote House Office until June 2021.

Due to the configuration of the system, payments could only be reviewed by two Senior Administrators after the payment was set up in the system, meaning that we were unable to evidence the effective operation of this control.

We note that RSM's testing has found that the sample of payments reviewed matched the payments processed, with no issues identified. We are therefore satisfied that this issue presented limited risk to our clients.

The Bristol Cote House office moved to our central payments procedures using CashFac from July 2021, which are outlined in control sections 2.3 and 4.2, and the NatWest Banking Online system is no longer in use.

2.3.7b Control

Increases are applied as confirmed by legislation. A copy of the increases to be applied is retained on file.

An Administrator (Associate or above) updates and signs off the Pension Increase checklist or workflow with a Senior Administrator (Consultant or above) or another Administrator deemed competent by Management, completing a final sign off. Where a workflow is used, an audit trail is retained within the system as evidence of authorisation.

Exception noted

For a sample of schemes, confirmed increases were applied as confirmed by legislation. Inspected and confirmed a copy of the increases to be applied was retained on file.

Confirmed an Administrator (Associate or above) updated and signed off the Pension Increase checklist, however it was noted that there was no independent review in place to check the pension increase runtime parameters and that the final sign off as stated in the control was not formally documented, therefore, an exception was noted.

Management response

Pension increases in the Middlesbrough office are carried out using the Aquila Heywood Altair application through a bulk calculation routine.

Due to the way this application is configured, there is no inbuilt checking stage within the application after pension increase runtime parameters are input. Therefore we have not been able to evidence the independent checks carried out on the runtime parameters input.

Going forwards, in order to maintain evidence for audit purposes, we have implemented a new process where a screenshot of the increase runtime parameters is taken before the run is initiated and emailed to a second member of staff for formal written approval.

We would note that increase calculations are checked at other stages of the process, as evidenced in the files provided, and that this issue relates solely to the input of pension increase runtime parameters.

3.4.2 Control

On a monthly basis, as part of the Contribution Process, unit holding information is extracted from the PAS via a securely linked access database or from Control Account information held within the PAS. The results of this are reconciled by the Administration Team against the Investment Manager Holdings with any differences identified being fully investigated, documented and if necessary ring-fenced until a cause for the difference is identified and can be resolved. Copies of any correspondence are retained on file as evidence. The Unit Reconciliation is reviewed by a Senior Administrator or above and a copy retained either on the file or electronically on the system. Completion and review of the Unit Reconciliation is reported in the monthly Managers Report where any issues are highlighted. The DC Investment Tracker is updated and reviewed at the Managers Meetings and documented on the Minutes to confirm review. See 6.2.1

Exception noted

For a sample of DC schemes, across a sample of months, confirmed that on a monthly basis, as part of the Contribution Process, that a unit holding reconciliation was performed by the Administration team.

Confirmed differences identified were investigated and copies of correspondences were retained on file to evidence this.

Whilst it was confirmed that the Unit Reconciliation was performed, it was not evident, in all instances, that these had been reviewed by a Senior Administrator or above as this was not documented. As the control had not operated as described for the full reporting period, an exception is noted.

Management response

During 2021 we began the process of transferring many of our unit reconciliations to a central unit reconciliation team, with a small number continuing to be carried out by administration teams. Whilst building the central team and implementing the new reconciliation process we have noted there was unfortunately no formal process in place for unit reconciliations to be prepared and checked by two independent members of staff. A formal checking process has been implemented with effect from September 2021 and RSM have noted that this process was working effectively.

Completion of unit reconciliations is reported to management on a monthly basis, with any issues flagged and management therefore have oversight of their completion.

We believe that this posed a low level of risk, as we have processes in place to ensure that any issues with unit reconciliations are resolved each month and that the reconciliations are reported to Management each month.

7.2.7 Control

Network User Accounts: Change Requests to change user accounts are submitted to the IT Services Helpdesk by a business representative and actioned upon authorisation from the XPS IT Management.

Exception noted

A suitable system-generated or manually maintained population for this control was unable to be obtained for sampling. As such, this control could not be tested, therefore an exception is noted.

Management response

As we did not have a formally documented movers process in place during 2021, we were unable to provide RSM with a suitable system generated population of requests to change user accounts during the audit period.

Whilst we were able to provide a population of account changes to RSM through lists provided by our HR Team, we note that significant manual alterations and explanations were required to these lists, meaning that RSM were unable to gain confidence that an accurate list of user account changes had been provided.

We are currently implementing a new process through our HR Team and ServiceNow IT Helpdesk, which will enable us report more easily on requests to change user accounts. We expect this process to be implemented by the end of Quarter 2 2022.

7.2.8 Control

Notifications of terminated employees are sent to the IT Services Helpdesk by a business representative upon completion of a leaver form. The user accounts are either disabled immediately, if the termination date has passed and no authorisation to remain has been agreed or, with business authorisation, remain active for an agreed period after which time the account is closed.

Exception noted

For a sample of leavers, inspected the service desk ticket raised.

For three of the leavers tested, no corresponding ticket or form was able to be provided.

Noted from enquiry with management that changes to the internal processes for this control were made during the in-scope period. No exceptions were noted for sampled leavers with leave dates after these changes were made.

Management response

We were unable to locate evidence of a request being sent to remove access to the XPS IT network with relation to 3 of the 25 employees reviewed.

We have noted that access was removed in a timely manner upon these employees leaving XPS.

In 2 of the 3 cases the last logon date was prior to the users' leave dates and therefore this access was not exploited. In 1 case the last logon date was 1 day after the leave date, however we are satisfied that appropriate permission had been granted to the user to login on this date to complete outstanding tasks.

In addition to our standard leaver process, we carry out checks on a weekly basis to ensure that access has been removed appropriately, with an emergency leaver form issued where access had not been removed. Access was removed through this process, for 6 of the 25 leavers sampled.

We have implemented a new system-integrated leaver form, with effect from October 2021. We have noted that the above exceptions relate to the period prior to this process. RSM have carried out additional testing following the implementation of our new process, and found no exceptions to this process post-October 2021.

We are also currently carrying out an internal audit of all company leavers during Quarter 1 2022, to ensure that access has been removed appropriately and that our new process is functioning effectively.

Service Auditor Report



RSM Risk Assurance Services LLP

25 Farringdon Street
London
EC4A 4AB
T +44 (0)20 3201 8000
F +44 (0)20 3201 8001
rsmuk.com

Our ref: JT/01-20/2021

Strictly Private & Confidential
REASONABLE ASSURANCE REPORT

The Directors
XPS Administration Limited
11 Strand
London
WC2N 5HR

4 May 2022

Dear Sirs

INDEPENDENT ASSURANCE REPORT ON INTERNAL CONTROLS OF SERVICE ORGANISATION

This report is made solely for the use of the Directors, as a body, of XPS Administration Limited (herein XPS) ('the Service Organisation'), and solely for the purpose of reporting on the internal controls of the Service Organisation, in accordance with the terms of our engagement letter dated 20 May 2021.

USE OF SERVICE AUDITOR'S REPORT

Our work has been undertaken so that we might report to Senior Management those matters that we have agreed to state to them in this report and for no other purpose. The Service Auditor's report is released to the Service Organisation on the basis that it shall not be copied, referred to or disclosed, in whole or in part (save as otherwise permitted by agreed written terms), without our prior written consent.

The Service Auditor's Report is designed to meet the agreed requirements of the Service Organisation and particular features of our engagement determined by their needs at the time. The Service Auditor's report should not therefore be regarded as suitable to be used or relied on by any other party wishing to acquire any rights against RSM UK Risk Assurance Services LLP for any purpose or in any context. Any party other than the Service Organisation which obtains access to this report or a copy and chooses to rely on the Service Auditor's Report (or any part of it) will do so at its own risk. To the fullest extent permitted by law, RSM UK Risk Assurance Services LLP will accept no responsibility or liability in respect of this report to any other party and shall not be liable for any loss, damage or expense of whatsoever nature which is caused by any person's reliance on representations in this report.

We permit the disclosure of the Service Auditor's Report, in full only, to User Entities of the Service Organisation using the Service Organisation's Pension Administration services ('User Entities'), and to the auditors of such User Entities, to enable User Entities and their auditors to verify that the Service Auditor's Report has been commissioned by Senior Management of the Service Organisation and issued in connection with the internal controls of the Service Organisation without assuming or accepting any responsibility or liability to them on our part.

THE POWER OF BEING UNDERSTOOD AUDIT | TAX | CONSULTING

RSM UK Corporate Finance LLP, RSM UK Legal LLP, RSM UK Restructuring Advisory LLP, RSM UK Risk Assurance Services LLP, RSM UK Tax and Advisory Services LLP, RSM UK Audit LLP, and RSM UK Consulting LLP and Baker Tilly Creditor Services LLP are limited liability partnerships registered in England and Wales, with registered numbers OC325347, OC402439, OC325349, OC389499, OC325348, OC325350, OC397475 and OC398986 respectively. RSM Employer Services Limited, RSM UK Tax and Accounting Limited and RSM UK Management Limited are registered in England and Wales with numbers 6463594, 6677561 and 3077999 respectively. RSM Northern Ireland (UK) Limited is registered in Northern Ireland at Number One Lanyon Quay, Belfast, BT1 3LG with number NI642821. All other limited companies and limited liability partnerships are registered at 6th Floor, 25 Farringdon Street, London, EC4A 4AB. The UK group of companies and LLPs trading as RSM is a member of the RSM network. RSM is the trading name used by the members of the RSM network. Each member of the RSM network is an independent accounting and consulting firm which practises in its own right. The RSM network is not itself a separate legal entity in any jurisdiction.

RSM UK Legal LLP is authorised and regulated by the Solicitors Regulation Authority, reference number 626317.



SCOPE

We have been engaged to report on the Service Organisation's description of its Pension Administration activities throughout the period 1 January 2021 to 31 December 2021 (the description), and on the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description.

SERVICE ORGANISATION'S RESPONSIBILITIES

The Service Organisation is responsible for:

- preparing the description and the accompanying assertion set out on pages 1 to 25, including the completeness, accuracy, and method of presentation of the description and the Management assertion;
- providing the services covered by the description;
- specifying the criteria and stating them in the description;
- identifying the risks that threaten the achievement of the control objectives; and
- designing, implementing control activities to achieve the stated control objectives stated in the description.

The control objectives stated in the description on pages 33 to 36, include the internal control objectives developed for service organisations as set out in the ICAEW Technical Release AAF 01/20.

SERVICE AUDITORS' RESPONSIBILITIES

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design of the control activities and operating effectiveness of the controls to achieve the related control objectives stated in that description based on our procedures. We conducted our engagement in accordance with International Standard on Assurance Engagements 3000 and 3402, and ICAEW Technical Release AAF 01/20. Those standards and guidance require that we comply with ethical requirements and plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented and the control activities were suitably designed to achieve the related control objectives stated in the description, throughout the period 1 January 2021 to 31 December 2021.

Our work involved performing procedures to obtain evidence about the presentation of the description of the Pension Administration activities and the design and operating effectiveness of those controls. Our procedures included assessing the risks that the description is not fairly presented and that the control activities were not suitably designed or operating effectively to achieve the related control objectives stated in the description.

Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related control objectives stated in the description were achieved.

An assurance engagement of this type also includes evaluating the overall presentation of the description and the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organisation and described at pages 7 and 8.

INHERENT LIMITATIONS

The Service Organisation's description is prepared to meet the common needs of a broad range of User Entities and their auditors and may not, therefore, include every aspect of the Service Organisation Pension Administration activities that each individual User Entity may consider important in its own particular environment. Also, because of their nature, control activities at a service organisation may not prevent or detect and correct all errors or omissions in processing or reporting transactions or identification of the function performed by the service organisation or system.

Our opinion is based on historical information and the projection to future periods of any evaluation of the fairness of the presentation of the description, or opinions about the suitability of the design or operating effectiveness of the control activities would be inappropriate.



NON-APPLICABLE CONTROL OBJECTIVES

The scope of our engagement includes all control objectives and control activities included in the description with the exception of one in the section, Accepting Clients. Specifically, we did not perform any procedures over the control activity in relation to the following control objective:

- Opening balances for client take-ons are completely and accurately recorded and communicated to clients in line with client instructions.

since Management confirmed that there had been no new DC clients during the reporting period 1 January to 31 December 2021, therefore, the control in place for the above objective did not operate. Accordingly, we do not express an opinion thereon.

EXCEPTIONS TO OPERATING EFFECTIVENESS

Except for the matters explained on page 27 to 29 concerning the exceptions to operating effectiveness noted with respect to the control activities tested, as set out on pages 37 to 141 of the report by Senior Management, our opinion is as follows.

OPINION

In our opinion, in all material respects, based on the criteria described in the Service Organisations Management' Statement on pages 7 to 8:

- a) the description on pages 1 to 25 fairly presents the service organisation activities or system as designed and implemented throughout the period from 1 January 2021 to 31 December 2021;
- b) the control activities related to the control objectives stated in the description on pages 33 to 141 were suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described control activities operated effectively throughout the period from 1 January 2021 to 31 December 2021;
- c) the control activities tested, which were operating with sufficient effectiveness to provide reasonable assurance that the related control objectives stated in the description were achieved throughout the period 1 January 2021 to 31 December 2021.

DESCRIPTION OF TESTS OF CONTROLS

The specific controls tested and the nature, timing and results of those tests are detailed on pages 37 to 141.

To the fullest extent permitted by law, we do not accept or assume responsibility to anyone other than the Service Organisation for our work, for this report, or for the opinions we have formed.

We have no responsibility to update this letter for events and circumstances occurring after the date of this letter.

RSM UK Risk Assurance Services LLP

RSM UK Risk Assurance Services LLP

London

4 May 2022

Summary of Control Objectives

Ref	Control objectives
1	Accepting clients <ul style="list-style-type: none">› New client agreements and amendments are authorised prior to initiating pension administration activity.› Pension scheme member details and accounts are completely and accurately set up onto relevant systems in accordance with the scheme rules and individual elections.› Opening balances for client take-ons are completely and accurately recorded and communicated to clients in line with client instructions.
2	Authorising and processing transactions <ul style="list-style-type: none">› Contributions and transfers-in received, and where applicable allocation of members' funds to investment options are processed completely, accurately and within agreed timescales.› Switches of members' funds between investment options and other rebalancing transactions are processed completely, accurately and within agreed timescales.› Benefits payable and transfer values are calculated in accordance with scheme rules and relevant legislation and are paid within agreed timescales.
3	Maintaining financial and other records <ul style="list-style-type: none">› Member records consist of up-to-date and accurate information.› Requests to change member records are validated for authenticity.› 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.› Scheme documents are complete, up to date and securely held.
4	Safeguarding assets <ul style="list-style-type: none">› Member records are securely held and access is restricted to authorised individuals.› Cash in scheme bank accounts is safeguarded and payments are suitably authorised.

5 Managing and monitoring compliance and outsourcing

- › Receipts of contributions are monitored against required timescales.
- › Pension administration activities are governed by service level agreements that are authorised and subject to regular review. Service performance is regularly monitored and assessed against the standards set out in the service level agreements.
- › Transaction errors are identified, reported to clients and resolved in accordance with established policies.
- › Periodic reports to The Pensions Regulator and HMRC are complete and accurate.

6 Reporting to clients

- › Periodic reports to participants and scheme trustees are complete, accurate, and provided within required timescales.
 - › Annual reports and accounts prepared for pension schemes are complete, accurate and provided within required timescales.
-

Information Technology

Control objectives

Restricting access to systems and data

- › Physical access to in-scope systems is restricted to authorised individuals.
 - › Logical access to in-scope systems and data is restricted to authorised individuals in accordance with job roles and/or business requirements.
 - › Client and third party access to in-scope systems and data is restricted and/or monitored.
 - › Segregation of incompatible duties within and across business and technology functions is formally defined, implemented, updated and enforced by logical security controls.
-

Maintaining integrity of the systems

- › Scheduling and internal processing of data is complete, accurate and within agreed timescales.
 - › Transmission of data to/from external parties is complete, accurate, executed within agreed timescales and secured in line with external party agreements.
 - › Network perimeter security devices are installed and changes are tested and approved.
 - › Anti-virus definitions are periodically updated across all terminals and services, deployment and setting are periodically reviewed and updated when required; and patterns of attempted external breaches are monitored.
 - › Data received from external parties is scanned for known vulnerabilities, any compromised data is quarantined and definitions of threats are periodically updated.
-

Maintaining and developing systems hardware and software

- › Development and implementation of both in house and third party in-scope systems are authorised, tested and approved.
 - › Data migration or modification is authorised, tested and, once performed, reconciled back to the source data.
 - › Changes to existing in-scope systems, including hardware upgrades, software patches and direct configuration changes, are authorised, tested and approved in line with policy.
-

Recovering from processing interruptions

- › IT related Disaster Recovery Plans are documented, updated, approved and tested.
- › In-scope systems and data are backed up and tested such that they can be restored completely and within agreed timescales.
- › Problems and incidents relating to in-scope systems are identified and resolved within agreed timescales.

Managing and monitoring compliance and outsourcing

- › Outsourced activities provided by Subservice Organisations are governed by contracts and service level agreements that are authorised and subject to regular review.
 - › The services provided by Subservice Organisations are regularly monitored and assessed against the standards set out in the service level agreements.
-

Control Procedures and Service Auditor Tests

1. Accepting clients

1.1 New client agreements and amendments are authorised prior to initiating pension administration activity

1.1.1 Process

A tailored, client-specific administration agreement which includes an administration and data protection agreement is drawn up, reviewed and amended as required.

Control

Full administration services only commence once the administration contract has been signed by all contracting parties and not before the agreed administration Go Live date.

Auditor testing and results

For a sample of new schemes, obtained the corresponding Administration contract and confirmed that this had been signed by the contracting parties. Confirmed that the agreement was in place prior to go live.

No exceptions noted.

1.1.2 Process

An Administrator completes due diligence checks, including Anti-Money Laundering (AML) procedures as part of the initial client set up process. No appointment is accepted until the process is completed.

The scheme and sponsoring employer registration status are reviewed and retained on file.

Control

With the exception of existing clients where non administration services are provided within XPS Pensions Group, appointments are only accepted once AML checks have been completed. An XPS Administrator checks the registration status of the Scheme and sponsoring employer to ensure that they have regulatory approval. Proof of their status is retained on file.

Auditor testing and results

For a sample of new schemes confirmed that AML checks were performed. Confirmed XPS Administrator had checked the registration status of the Scheme and sponsoring employer to ensure that they have regulatory approval; and that this is retained on file.

No exceptions noted.

1.1.3 Process

The Client Banking team completes a form to open the bank account using information provided by the Client. A list of Authorised Client Representatives is obtained as part of the Scheme Implementation.

The application is signed by the trustees with a mandate granting signing rights to authorised signatories within XPS Administration and confirming payment authorisation limits.

Control

Scheme bank accounts are authorised for opening via written instruction from the Client prior to the account being opened. A copy of the written instruction to open an account and any related correspondence is retained on file.

Auditor testing and results

For a sample of new scheme bank accounts, confirmed that the client's written approval had been obtained prior to the account opening.

No exceptions noted.

1.1.4 Process

New scheme bank account details are sent by a Client Banking Administrator to the bank which confirms in writing once the account has been opened.

The Accounts Manager arranges for the scheme to be set up on the Accounting system using the details provided by the Client Banking Team. The Client Banking Team arranges for the bank account to be linked to the online banking portal.

Control

Following confirmation that the new bank account has been opened, the Client Banking Administrator will check the new bank account number. As part of the client take on process, the bank account is set up on the CashFac electronic banking platform and managed services are set up on the platform. The Administration Team Leader confirms the access permissions which should be granted on the CashFac system.

Auditor testing and results

For a sample of scheme bank accounts, confirmed that the Administrator Team Leader confirmed which access permissions should be granted on CashFac.

No exceptions noted.

1. Accepting clients

1.2 Pension scheme member details and accounts are completely and accurately set up onto relevant systems in accordance with the scheme rules and individual elections

1.2.1 Process

Following appointment, a 'handover period' is agreed with a date when full administration will commence.

All scheme data and documentation is requested from the current administrator.

A standard documentation checklist and scheme installation checklist are used to ensure that all relevant data and information is requested and all required stages of the migration process have been completed.

Control

The Pensions Administration Team or BSG (Business Services Group) use the documentation checklist to ensure that the correct information / data has been received. Items received are checked off against the data request form.

An installation checklist is completed by the Pension Administration Team to verify that all relevant administration stages of the migration project have been completed.

Auditor testing and results

For a sample of new schemes, inspected the installation checklist and confirmed this had been completed by the Pension Administration Team to confirm the relevant admin stages of the migration project had been completed.

No exceptions noted.

1.2.2 Process

Administration and Payroll (where applicable) data received is verified, reviewed and loaded by the supervisor.

Control

Penscope clients: Once the Administration Team Leader or Lead Administrator is satisfied that the data testing has been completed, a Migration Sign Off form is signed to confirm that data can be loaded to the Pensions Administration System (PAS). BSG and/or the Third Party Software provider arrange for the data to be loaded to the PAS and confirm to the Administration team once the scheme has been released to live.

Auditor testing and results

For a sample of new schemes, confirmed that the data Migration form had been completed and signed off prior to the data being loaded to PAS and set live.

Evidence of the confirmation of the scheme being set live from BSG/ a third party obtained.

No exceptions noted.

1.2.3 Process

Administration and Payroll (where applicable) data received is verified, reviewed and loaded by the System Analyst.

Control

Compendia clients: Once the BSG Technical Pensions Analyst is satisfied that the data testing has been completed, they confirm to the System Analyst in writing that the data can be loaded to the Pensions Administration System. The System Analyst formats the data and loads to the PAS.

Auditor testing and results

Enquired with management and confirmed that no new scheme take ons were set up on Compendia during the reporting period, therefore, no testing was undertaken. Management have confirmed the control remains as described.

1.2.4 Process

The BSG Team and/or the Client Team manage and monitor the client take on process.

A Project Initiation Document (PID) is drafted and agreed with the Client, confirming the key project deliverables, timescales and stakeholders.

Progress of the implementation is tracked through a Project Plan and reported on through Highlight Reports which are issued to clients or another communication strategy agreed for the project.

Control

Any issues identified during the project are logged by the BSG Project Manager in an Issue Log and resolved with the previous administrator or the sponsoring employer.

Once all stages have been completed the project is closed off by the Project Manager or the Lead Administrator, where appropriate by issue of a Project Closure Report.

Auditor testing and results

For a sample of new schemes, confirmed an error log was in place and that this was updated. Obtained the project closure report and confirmed this was issued by the Project Manager or Lead Administrator.

No exceptions noted.

1.2.5 Process

The client team define the calculation requirements and identify the methodology to be used for each scheme (Pensions Administration System, spreadsheet or calculation proforma).

Appropriate sections are set up on the Pensions Administration System to reflect the scheme rules and individual elections. Calculations are specified in accordance with the scheme rules.

Control

The client team defines the calculation methodology to be used for each scheme, including whether calculations need to be coded. Where calculations are coded, the methodology to be used is signed off by the Lead Administrator (System calculations, spreadsheet or calculation proforma).

Where calculations are coded calculation specifications for each section are created by the Client Team / BSG. These specifications are then signed off by the Lead Administrator or the Scheme Actuary (where specified by client).

A test pack of calculations is manually produced in accordance with the scheme rules and checked by the Team Leader or Lead Administrator and compared against the automated results produced by the pension administration system.

Once the Client Team / BSG have resolved any issues identified in testing the calculations are formally signed off by the Team Manager or Lead Administrator, with the results and signoff retained on file. Calculations are then released for used in the Live Environment.

Auditor testing and results

For a sample of new schemes, where calculations were coded, confirmed the methodology to be used was signed off by the Lead Administrator (System calculations, spreadsheet or calculation proforma).

Inspected the test pack of calculations manually produced in accordance with the scheme rules and confirmed checked by the Team Leader or Lead Administrator and compared against the automated results produced by the pension administration system.

Confirmed testing the calculations were formally signed off by the Team Manager or Lead Administrator, with the results and signoff retained on file. Confirmed that release for use in the Live Environment was post approval.

No exceptions noted.

1. Accepting clients

1.3 Opening balances for client take-ons are completely and accurately recorded and communicated to clients in line with client instructions

1.3.1 Process

Defined Contribution (DC) records are set up to mirror totals held by the previous administrator in accordance with individual elections.

Control

Fund monetary totals are reconciled to the previous administrators' totals for each investment fund, and individual records spot-checked by a DC Senior Administrator (Consultant or above) or another DC Administrator deemed competent by Management. Any differences or anomalies (including negative unit holdings for individual members and positive unit holdings for members who have left the scheme) are identified and corrective action is taken as necessary.

Auditor testing and results

Enquired with management and confirmed that there were no new DC scheme take ons during the reporting period, therefore, no testing was undertaken. Management have confirmed the control remains as described.

2. Authorising and processing transactions

2.1 Contributions and transfers-in received, and where applicable allocation of members' funds to investment options are processed completely, accurately and within agreed timescales

2.1.1 Process

The DC Contributions checklist provides guidance for the administration team when collecting, investing and allocating monthly contributions.

Control

On a monthly basis the DC Administration team use the Contributions Checklist as a guide to contribution processes. The workflow is completed and updated at each stage of the investment process by an Administrator (Associate or above) and checked by a Senior Administrator (Consultant or above) or another Administrator deemed competent by Management. An audit trail is retained within the PAS as evidence.

Auditor testing and results

Enquired with management and confirmed that there were no new DC scheme take ons during the reporting period, therefore, no testing was undertaken. Management have confirmed the control remains as described.

No exceptions noted.

2.1.2 Process

Data confirming monthly contributions is received electronically from the client in a pre-agreed format and loaded onto the PAS by the DC Administration Team. The PAS automatically highlights any changes to member information, which are queried with the client where appropriate.

The PAS generates summary investment instructions based on the contributions received and investment instructions held on behalf of each member.

The DC Administration Team reconciles contribution amounts between the PAS and the file received from the client, taking into account any amendments agreed with the client to ensure that the match. Any differences are queried with the client and resolved before the file is loaded.

Control

On a monthly basis the DC Administration Team reconciles contribution totals between the PAS, the contribution file received from the Employer and the money received into the Scheme bank account.

Any differences are queried and once they have been resolved the contributions file is uploaded to the PAS and a clear validation report is printed and retained on file.

The contributions checklist and workflow are completed by an Administrator (Associate or above) and checked by a Senior Administrator (Consultant or above) or another Administrator deemed competent by Management, including the amount of the contribution received and to show that the contributions have been reconciled.

Auditor testing and results

For a sample of schemes and a sample of months, confirmed that the DC Admin team had reconciled the contributions to the PAS and contributions received in the scheme bank accounts.

Confirmed that queries were followed up and inspected the validation report to confirm this was retained.

Inspected the contributions checklist and workflow and confirmed this was completed by an Administrator (Associate or above) and checked by a Senior Administrator (Consultant or above) or another Administrator deemed competent by Management.

No exceptions noted.

2.1.3 Process

The DC Administration Team obtains confirmation of investment prices and total units purchased from the Investment Manager. The DC Administration Team update the PAS with the unit prices provided and the control accounts with the total number of units purchased in each fund.

The PAS calculates and updates each of the Member's records with the units purchased.

Control

On a monthly basis the DC Administration Team verifies the total investment amount confirmed by the Investment Manager matches the original investment instructions. Any discrepancy is immediately raised with the Investment Manager for investigation and resolution.

Once any differences are resolved the contributions checklist is completed and signed off by two independent DC Administration Team members or the workflow is completed and authorised as evidence of completion of the contributions process.

Auditor testing and results

For a sample of DC schemes, across a sample of months, confirmed the investment totals had been agreed by the DC Administration Team. Where differences, confirmed these had been investigated and resolved. Inspected the contribution checklist and confirmed this had been completed and signed by two independent DC Administration team members.

No exceptions noted.

2.1.4 Process

DC transactions and DB transfers-in

Individual DB transfers-in and DC transactions are initiated on receipt of appropriate authorised instructions from the Member, or the Scheme Trustees. Workflows and/or checklists are used as guidance to carry out DB or DC transactions based on the type of transaction being completed. These confirm that the correct process has been followed and that the work has been authorised as complete within the SLA guidelines.

Control

DB transfers-in and DC transactions are signed off by an Independent Administrator using the checklist or workflow in place for the specific type of these transactions. The Administrator checks that all required workflow steps have been completed in accordance with member or client instructions. An Administrator signs off the Checklist and/or authorises the workflow in the PAS. This retained in the system as evidence of authorisation and completion of the task.

Auditor testing and results

For a sample of transfers-in and transactions inspected the checklist / workflow in place and confirmed this was signed off by an Independent Administrator.

Inspected the workflow and confirmed evidence of authorisation and completion of the task.

No exceptions noted.

2.1.5 Process

DC transactions

The Administration Team complete instructions detailing the number of units to be bought or sold. This is authorised from a list of authorised signatories from the Investment Mandate agreed with the Scheme Trustees. If a unit purchase is being made, the Administration Team arrange for cash to be transferred to the Investment Manager, which is signed in accordance with section 4.2 regarding payment safeguarding and authorisation.

Control

The unit purchase or sale instruction is authorised in accordance with the Scheme’s Investment Mandate, from a list of authorised signatories agreed with the Scheme Trustees prior to sending to the Investment Manager. Where a unit purchase is required the instruction to transfer cash to the Investment Manager is signed in accordance with the Investment Mandate as per Control section 4.2.

Auditor testing and results

For a sample of unit purchases or sale instructions, inspected evidence and confirmed these had been authorised in line with authorised signatories of Scheme Investment Mandate.

No exceptions noted.

2.1.6 Process

DC Transactions

Once the instruction is executed, the Investment Manager processes the unit transaction and sends details to the Administration Team. The Administration Team checks that the confirmation received from the Investment Manager matches the instructions submitted and updates the PAS with appropriate details. Any differences to the instruction submitted are queried with the Investment Manager.

Control

On receipt of the Contract Note from the Investment Manager, an administrator (Associate or above) updates the PAS with details of the trade. An independent administrator (Consultant or above) or another Administrator deemed competent by Management verifies that the PAS has been updated and authorises the workflow or completes the checklist.

Auditor testing and results

For the same sample of instructions in 2.1.5, noted that the PAS had been updated with detail of the trade by an Administrator and reviewed by an independent Administrator. Confirmed that the workflow had been authorised or checklist completed to document review.

No exceptions noted.

2.1.7a-2.1.8a Process

Non-Bristol Cote House

Where XPS Administration administers the scheme bank account, on a monthly basis or other frequency agreed with the Client, a DB Pensions Administrator prepares a Cash Flow Forecast detailing the expected expenses and receipts over the next month. The Cash Flow Forecast is populated with the opening cash balance, transactions and the closing balance from the Client Banking system. Cash Flows are also reported to Clients as required.

Control

2.1.7a A Pensions Administrator (Associate or above) prepares a Cash Flow Forecast, detailing the cash requirement for the following month and signs the forecast as prepared. A Senior Administrator (Consultant or above) or an Administrator deemed competent by Management independently reviews the forecast for accuracy and signs as reviewed.

Auditor testing and results

For a sample of schemes across a sample of months, inspected the cashflow forecast and confirmed this had been prepared by an Administrator. Confirmed a Senior Administrator (Consultant or above) or an Administrator deemed competent by Management independently reviewed the forecast and signed as reviewed.

No exceptions noted.

Control

2.1.8a Where agreed, the cashflow is sent to the client to confirm whether an investment or disinvestment of funds is required. If any investment or disinvestment is required, an instruction is prepared to the investment manager which is signed off in line with the signatory mandate.

Auditor testing and results

For a sample of schemes across a sample of months, where agreed with the client, confirmed the cashflow was sent to the client to confirm whether an investment or disinvestment of funds was required.

Where investment or disinvestment was required, confirmed an instruction was prepared in line with the signatory mandate.

No exceptions noted.

2.1.7b-2.1.8b Process

Bristol Cote House

Where XPS Administration administers the scheme bank account, on a monthly basis or other frequency agreed with the Client, a Treasury Administrator prepares a Cash Flow Forecast detailing the expected expenses and receipts over the next month or agreed review period. The Cash Flow Forecast is populated with the opening cash balance, transactions and the closing balance from the Client Banking system. Cash Flows are also reported to Clients as required.

Control

2.1.7b An Administrator (Associate or above) prepares a Cash Flow Forecast, detailing the cash requirement for the following month or other agreed period and signs the forecast as prepared. A Senior Administrator (Consultant or above) or an Administrator deemed competent by Management independently reviews the forecast for accuracy and signs as reviewed.

Auditor testing and results

For a sample of months and a sample of schemes, it was noted that the cashflows were prepared by an Administrator and reviewed by an independent Senior Administrator.

No exceptions noted.

Control

2.1.8b Where agreed, the cashflow is sent to the client to confirm whether an investment or disinvestment of funds is required. If any investment or disinvestment is required, an instruction is prepared to the investment manager which is signed off in line with the signatory mandate.

Auditor testing and results

For a sample of schemes across a sample of months, where agreed with the client, confirmed the cashflow was sent to the client to confirm whether an investment or disinvestment of funds was required.

Where investment or disinvestment was required, confirmed an instruction was prepared in line with the signatory mandate.

No exceptions noted.

2.1.8 Process

Client 435 only

On a monthly basis, a three month cashflow forecast is completed by an accountant, using standard round figures copied from a template. The current bank balance from the accounts system is used to prepare the forecast. Funds are invested/disinvested by the client as per the cashflow results.

Control

Standard round figures are used as agreed with the client, which are copied from a template. The current bank balance from the accounts system along with known forthcoming events is used to prepare a quarterly forecast which is sent to the client. Any differences are resolved before the forecast is issued to the client.

Once the client receives the Cashflow reports the necessary investment/ disinvestment will be actioned by the client as required.

Auditor testing and results

For a sample of months, for client 435, confirmed that a quarterly forecast was prepared and sent to the client.

For the months tested, no investment/ disinvestments were required to be actioned by the client. Management confirmed the control remains as described.

No exceptions noted.

2. Authorising and processing transactions

2.2 Switches of members' funds between investment options and other rebalancing transactions are processed completely, accurately and within agreed timescales

2.2.1 Process

At least annually, a workflow is launched to carry out lifestyle switches. The DC Administration Team identifies any Members due for lifestyle switches and calculates their lifestyle trades in line with scheme documentation.

The DC Administration team send the lifestyle investment instructions and investment amounts to the Investment manager. Once the lifestyle switches have been made, the DC Administration team update the PAS with details confirmed by the Investment Manager.

A Lifestyling checklist is used to guide to the process.

Additional monitoring occurs to ensure that lifestyle switches across all Schemes are updated within the required timescales as defined in the SLA.

Control

At least annually an Administrator (Associate or above) identifies any Members due for lifestyle switches and calculates their lifestyle trades in line with scheme documentation either manually or using an individual or bulk automated system process. A Senior Administrator (Consultant or above) or another Administrator deemed competent by Management reviews the lifestyle calculations before they are sent to the investment manager.

Once the lifestyle trade has been made, the DC Administration team check that the trade instruction received from the Investment Manager matches the original request and update the PAS with details confirmed by the Investment Manager.

A Lifestyling checklist or the automated PAS tasks are used to guide the process. Completion of the task is evidenced by completion of a checklist or authorisation of a workflow or authorisation through the automated PAS process.

An audit trail is retained in the PAS as further evidence of authorisation.

Auditor testing and results

For a sample of DC schemes, confirmed that at least annually an Administrator identified Members due for lifestyle switches and calculated lifestyle trades in line with scheme documentation either manually or using an individual or bulk automated system process. Confirmed a Senior Administrator or another Administrator deemed competent by Management reviewed the lifestyle calculations before they were sent to the investment manager.

Inspected the checklist and confirmed the DC Administration team checked that the trade instruction received from the Investment manager matched the original request and updated the PAS with details confirmed by the Investment Manager.

Confirmed a Life styling checklist/automated PAS tasks was used to guide the process and that completion of the task was evidenced through completion of the checklist or authorisation of a workflow or authorisation through the automated PAS process.

No exceptions noted.

2.2.2 Process

Each month the DC Investment Tracker is reviewed by a Manager/ Team Leader or Senior Administrator (Consultant or above) or another Administrator deemed competent by Management to verify that the lifestyling investment has been performed correctly and within SLA.

A unit reconciliation is carried out to verify that the unit holding on the PAS matches the Investment Manager fund Valuation.

Control

The progress of the lifestyle process is monitored by the DC Administration Team on a monthly basis or at a frequency agreed with the Client using a tracking log.

Any Investment that fails to meet the Client SLA is reported immediately to the Client. The Administration Team prepares and sends the Client a loss assessment, if appropriate.

Auditor testing and results

Inspected the DC tracking log and confirmed progress of the lifestyle process is monitored by the DC Administration Team on a monthly basis or at a frequency agreed with the Client using a tracking log.

For the samples tested there were no Investments that failed to meet the Client SLA, therefore, confirmed with management that the control remains as described.

No exceptions noted.

2. Authorising and processing transactions

2.3 Benefits payable and transfer values are calculated in accordance with scheme rules and relevant legislation and are paid within agreed timescales

2.3.1 Process

XPS Administration is informed of an event leading to a benefit payment by the Client's payroll, HR, the Member, or an authorised third party, either by e-mail, hard copy notification or by an automated monthly client interface file. Notification of normal retirement is generated automatically by the PAS.

On a daily basis a Pensions Administrator creates a case for the benefit payment in a workflow system. The workflow system allocates a Service Level Agreement date (SLA) based on the case type created, which is hard coded into the workflow system.

Benefits calculated are checked for accuracy and completeness against the source documentation (i.e. hard copy of benefit payment details or scanned in equivalent) prior to making any payment.

The Administration Team use an automated workflow built into the PAS or a Control Sheet to guide the benefit process. Both automated workflows and Control Sheets include all process steps required to calculate a benefit in compliance with applicable Legislation and Scheme Rules.

Benefit calculations are either automated in the PAS, supported by Proformas signed off by the Scheme Actuary or Scheme Representative or performed manually. Where a calculation is performed manually a Pensions Administrator follows the calculation process described in either the Proforma or with direct reference to the Scheme Rules and any Rule Amendments. Benefit calculations are checked by a Senior Administrator (Consultant leave) or above, or another Administrator deemed competent by Management, where required to ensure accuracy.

Control

Benefit calculations are reviewed by a Senior Administrator (Consultant level or above) or another Administrator deemed competent by Management.

Where Proformas are in place, the review may be through verification to confirm they have been signed off by a Scheme Actuary or Scheme Representative and accurately implemented into the PAS.

For Manual benefit calculations, a second Pensions Administrator reviews the calculation against either the Proforma or the Scheme Rules to verify that the calculation has been done correctly and signs the calculation as evidence of this review.

Auditor testing and results

For a sample of benefit calculations, confirmed these were reviewed by a Senior Administrator (Consultant level or above) or another Administrator deemed competent by Management.

Where proformas were in place, confirmed signed off by a Scheme Actuary or Scheme Representative.

For manual benefit calculations, confirmed a second Pensions Administrator reviewed the calculation against either the Proforma or the Scheme Rules to verify that the calculation has been done correctly and signed the calculation as evidence of review.

No exceptions noted.

2.3.2a Process

Benefit payment workflows are signed off by a Senior Administrator (Consultant level or above) or another Administrator deemed competent by Management.

Once the workflow or Control Sheet is complete a payment is generated in the Client Cash Management (CCM) system. All individual payments are checked and authorised in line with the XPS signatory mandate and the Scheme bank mandate before being released.

Control

A Senior Administrator (Consultant level or above) or another Administrator deemed competent by Management validates that all of the workflow steps and associated processes, (for example benefit calculations, member authorisation to proceed etc.) have been performed correctly using the process checklist as a guide. The workflow is authorised in the PAS, and an audit trail is retained within the PAS as evidence of authorisation.

Auditor testing and results

For a sample of benefit payments, confirmed a Senior Administrator (Consultant level or above) or another Administrator deemed competent by Management validated that all of the workflow steps and associated processes had been performed correctly in line with the process checklist. Confirmed the workflow was authorised in the PAS, and an audit trail was retained within the PAS as evidence of authorisation.

No exceptions noted.

2.3.2b Process

Altair schemes only

An Administrator creates the Payroll record manually (non-public sector schemes) or this is created automatically by the Altair system (public sector schemes only).

Control

A Senior administrator (Consultant level or above) or another Administrator deemed competent by Management validates that all appropriate steps have been taken and the benefits are being set up correctly by the Administrator and approves the Payroll record in the Altair system. This generates the payroll elements and records for the pension to be paid.

Auditor testing and results

For a sample of benefit payments, confirmed a Senior administrator (Consultant level or above) or another Administrator deemed competent by Management approved the Payroll record in the Altair system.

No exceptions noted.

2.3.3 Process

Client 430 only

Where benefits are payable a diary note is set up to arrange for settlement. A fund request is sent to the client through the CashFac system to provide funds to settle the members benefits on a daily basis.

Control

On a daily basis where required a fund request is sent to the client by the Client Banking Team to request funding for benefit settlements. The fund request is subject to standard authorisation processes (see Control 4.2.5) before being released to the client.

Auditor testing and results

For a sample of days, confirmed that email requests were sent by the Client Banking Team to Client 430. For a sub-sample of fund requests, confirmed these were approved prior to release to the client.

No exceptions noted.

2.3.4 Process

Discretionary benefit payments require Trustee approval prior to executing the payment. For certain payments i.e. pension commencement lump sums, a 'blanket' approval exists allowing payment to proceed without Trustee approval for each case.

Control

Where Trustee approval is required, the Senior Pensions Administrator (Consultant level or above) or another Administrator deemed competent by Management verifies that a copy of Trustee approval has been obtained, printed and filed, prior to signing off the workflow and/or Control Sheet. Where authorisation is part of a workflow, an audit trail is retained within the system as evidence of authorisation.

Auditor testing and results

For a sample of discretionary payments, confirmed where Trustee approval was required, that the Senior Pensions Administrator (Consultant level or above) or another Administrator deemed competent by Management verified that a copy of Trustee approval has been obtained, printed and filed, prior to signing off the workflow and/or Control Sheet.

No exceptions noted.

2.3.5a Process

One off payments and first pensioner payments are initiated and authorised by Pensions Administration and sent to the Payroll Team. A pension record is created on the Payroll System for one off or subsequent regular pension payments.

The Payroll Team run a Payroll Reconciliation Report prior to payroll run.

A Payroll administrator reviews movements identified on the Payroll Reconciliation Report e.g. manually input New Pensioners, pensioner amendments, pensions ceasing, to make sure they are consistent with their understanding of the scheme and also with movements processed by the Pensions Administration Team during the month. New Pensioners imported via the workflow are recorded as a total.

The Payroll Book, which identifies changes to the payroll over the month (e.g. new pensioners, pensioners who have died, etc.), is used to confirm that all differences can be explained. Totals from the payroll book are recorded on the Reconciliation Sheet and the Payroll Team checks the reconciliation for accuracy. Any discrepancies are resolved within the Payroll Team.

Once the payroll has been authorised a copy of the Authorisation Form is sent to the Pensions Administration and Client Banking teams. The total payroll payment is added to CashFac as an Expected Payment and transmitted through payroll software.

Control

On a monthly basis, the Payroll Team reconciles all differences between the previous month's payroll and the current month's payroll. Copies of the current to previous month's payroll reconciliation report are retained by the Payroll Team.

The Payroll Administrator reviews the Payroll Reconciliation Report against payment details received from the Pensions Administrator to confirm all payment additions, deletions and modifications are included in the upcoming payroll payment run. Any inconsistencies are investigated within the Payroll Team and corrected where required. A Senior Payroll Administrator (Consultant or above) authorises the payroll reconciliation once all inconsistencies have been resolved. Any correspondence relating to the resolution of discrepancies is retained within the reconciliation file. An audit sample is taken each month to ensure that changes have been made correctly.

Once the payroll has been authorised a copy of the authorisation form is sent to the Pensions Administration and Client Banking teams. Where CCM is used the total payroll payment is added to CCM as an Expected Payment and transmitted through payroll software. Where CCM is not used an Administrator completes a Cashflow to ensure that sufficient funds are held in the Client bank account and a BACS payment is drawn directly from the Client bank account.

A sample of changes is independently reviewed each month across different clients by the payroll team, to ensure that changes have been applied correctly.

Auditor testing and results

For a sample of schemes, across a sample of months, confirmed that the Payroll Team reconciles differences between the previous month's payroll and the current month's payroll.

Inspected the Payroll Reconciliation Report against payment details received from the Pensions Administrator to confirm all payment additions, deletions and modifications were included in the upcoming payroll payment run.

Confirmed inconsistencies are investigated within the Payroll Team and corrected where required.

Confirmed a Senior Payroll Administrator (Consultant or above) authorised the payroll reconciliation once all inconsistencies have been resolved.

Inspected the audit sample taken in the month to ensure that changes have been made correctly.

Confirmed that once the payroll had been authorised, copy of the authorisation form is sent to the Pensions Administration and Client Banking teams.

Confirmed that where CCM was used, the total payroll payment is added to CCM as an Expected Payment and transmitted through payroll software. Where CCM is not used, confirmed an Administrator completed a Cashflow to ensure that sufficient funds are held in the Client bank account and a BACS payment is drawn directly from the Client bank account.

Confirmed a sample of changes is independently reviewed each month across different clients by the payroll team, to ensure that changes have been applied correctly.

No exceptions noted.

2.3.5b Process

Altair non-Public Sector schemes

One off payments and first pensioner payments are input to the PAS by the Pension Administration team who create a record in the PAS for one off or subsequent regular pension payments (see Control 2.2.2).

The Payroll Administrator reviews the PAS to confirm all payment additions, deletions and modifications are included in the upcoming payroll payment run. Any inconsistencies are investigated within the Payroll Team and corrected where required.

A Payroll administrator reviews movements identified on the PAS e.g. manually input New Pensioners, pensioner amendments, pensions ceasing, to make sure they are consistent with their understanding of the scheme and also with movements processed by the Pensions Administration Team during the month.

Control

The Payroll Administrator reviews the PAS to confirm all payment additions, deletions and modifications are included in the upcoming payroll payment run. Any inconsistencies are investigated within the Payroll Team and corrected where required.

A Senior Payroll Administrator (Consultant or above) authorises the payroll reconciliation once all inconsistencies have been resolved and signs off a checklist to confirm that the payroll has been agreed and approves the BACS payment to be drawn from the client bank account.

Auditor testing and results

For a sample of schemes and sample of months, confirmed that a reconciliation had been performed against the prior month's payroll by a member of the Payroll Team and that an independent member of the Payroll Team had checked the movements and evidenced this in the monthly checklist, and that the BACS payment had been approved and made after this check had been performed.

No exceptions noted.

2.3.5c Process

Profund

A Pension administrator reviews movements identified on the Payroll Reconciliation Report e.g. manually input New Pensioners, pensioner amendments, pensions ceasing, to make sure they are consistent with their understanding of the scheme and also with movements processed by the Pensions Administration Team during the month. New Pensioners imported via the workflow are recorded as a total.

Control

Once the Scheme Payroll has been processed, the Administrator reviews, for accuracy, the total amount on the BACS Confirmation Report against the sum total of the payroll files recorded on the CCM/Bankline.

Once the BACS and summary report has been reviewed, it is signed as checked by the Senior Administrator on the Monthly Pensioner Payroll Checklist to show review and completion, and saved in the relevant client folder for each tax period and year.

Note – Control effective until June 2021.

Auditor testing and results

For a sample of schemes and a sample of months, confirmed that once the Scheme Payroll has been processed, the Administrator reviewed, for accuracy, the total amount on the BACS Confirmation Report against the sum total of the payroll files recorded on the CCM/Bankline.

Inspected the BACS and summary report that had been reviewed, and confirmed signed as checked by the Senior Administrator on the Monthly Pensioner Payroll Checklist to show review and completion, and that this had been saved in the relevant client folder for each tax period and year.

No exceptions noted.

2.3.6a Process

Non-Profund

The payroll BACS file, detailing pension payments to be made electronically, is sent to the bank through C-Series for them to process payroll payments to individual pensioners. A confirmation report is produced when the file is successfully sent to verify that the number of files processed agrees with the amount sent. A summary report for every file submitted is printed and initialled to show that the submission has been completed.

Control

Once the Scheme Payroll has been processed, the Payroll Team reviews, for accuracy, the total amount on the BACS Confirmation Report against the sum total of the payroll files recorded on the Payment Services website. Once complete, the BACS submission checklist is signed and retained by the Payroll Team.

Once the summary report has been reviewed, it is signed as checked on the Monthly Pensioner Payroll Checklist to show review and completion and saved in the relevant client folder for each tax period and year.

Auditor testing and results

For a sample of schemes and a sample of months, confirmed the Scheme Payroll has been processed and that the Payroll Team reviewed the BACS Confirmation Report against the sum total of the payroll files recorded on the Payment Services website. Inspected the BACS submission checklist and confirmed this was signed and retained by the Payroll Team.

Confirmed the summary report had been reviewed, and that this was evidenced through as checked on the Monthly Pensioner Payroll Checklist. Confirmed saved in the relevant client folder for each tax period and year.

No exceptions noted.

2.3.6b Process

Profund

A payment output file is downloaded from the PAS and loaded to the Banking Online system in order to make payments.

Control

The payment output file is downloaded from the PAS by an Administrator for payment. This then follows the standard payment process (see control 4.2.3d).

Note – Control in operation until June 2021.

Auditor testing and results

For a sample of schemes and payments, due to the set up of the NatWest Banking system for payment, review by two Senior Administrators occurs after the payment is set up in the system for payment, therefore, an exception is noted.

The control cannot be evidenced as described due to the NatWest set up. It was noted that for the sample of payments reviewed, these matched payment processed.

Exception noted.

Management response:

The NatWest Banking Online system is a legacy system which was used in our Bristol Cote House Office until June 2021.

Due to the configuration of the system, payments could only be reviewed by two Senior Administrators after the payment was set up in the system, meaning that we were unable to evidence the effective operation of this control.

We note that RSM's testing has found that the sample of payments reviewed matched the payments processed, with no issues identified. We are therefore satisfied that this issue presented limited risk to our clients.

The Bristol Cote House office moved to our central payments procedures using CashFac from July 2021, which are outlined in control sections 2.3 and 4.2, and the NatWest Banking Online system is no longer in use.

2.3.7a Process

Pensions Increases

At least annually, or more frequently where specified, pension increases are calculated and applied based on the Scheme Rules and applicable Regulatory and Legislative practice, or as notified in writing by the Scheme Trustees.

The process is completed within contractually agreed timescales and in line with the Scheme Rules and applicable Legislation. The Pension Increase checklist or workflow is updated by an Administrator (Associate or above) and signed off by a Senior Administrator (Consultant or above) or another Administrator deemed competent by management.

Control

At least annually, or more frequently where specified, the DB Administration Team confirms any discretionary increases to be applied with an authorised Trustee representative. A copy of the Trustee approval is retained on file as evidence of verification.

An Administrator (Associate or above) updates and signs off the Pension Increase checklist or workflow with a Senior Administrator (Consultant or above) or another Administrator deemed competent by Management, completing a final sign off. Where a workflow is used, an audit trail is retained within the system as evidence of authorisation.

Auditor testing and results

For a sample of schemes, at least annually, inspected the Pension Increase checklist or workflow and confirmed the DB Administration Team applied any discretionary increases.

Confirmed an Administrator (Associate or above) updated and signed off the Pension Increase checklist or workflow with a Senior Administrator (Consultant or above) or another Administrator deemed competent by Management, completing a final sign off. Where a workflow was used, confirmed an audit trail was retained within the system as evidence of authorisation.

No exceptions noted.

2.3.7b Process

Altair Public Sector Pensions Increases

At least annually, or more frequently where specified, pension increases are applied as confirmed by legislation. The process is completed within contractually agreed timescales and in line with the applicable Legislation. The Pension Increase checklist or workflow is updated by an Administrator (Associate or above) and signed off by a Senior Administrator (Consultant or above) or another Administrator deemed competent by management.

Control

Increases are applied as confirmed by legislation. A copy of the increases to be applied is retained on file.

An Administrator (Associate or above) updates and signs off the Pension Increase checklist or workflow with a Senior Administrator (Consultant or above) or another Administrator deemed competent by Management, completing a final sign off. Where a workflow is used, an audit trail is retained within the system as evidence of authorisation.

Auditor testing and results

For a sample of schemes, confirmed increases were applied as confirmed by legislation. Inspected and confirmed a copy of the increases to be applied was retained on file.

Confirmed an Administrator (Associate or above) updated and signed off the Pension Increase checklist, however it was noted that there was no independent review in place to check the pension increase runtime parameters and that the final sign off as stated in the control was not formally documented, therefore, an exception was noted.

Exception noted.

Management response:

Pension increases in the Middlesbrough office are carried out using the Aquila Heywood Altair application through a bulk calculation routine.

Due to the way this application is configured, there is no inbuilt checking stage within the application after pension increase runtime parameters are input. Therefore we have not been able to evidence the independent checks carried out on the runtime parameters input.

Going forwards, in order to maintain evidence for audit purposes, we have implemented a new process where a screenshot of the increase runtime parameters is taken before the run is initiated and emailed to a second member of staff for formal written approval.

We would note that increase calculations are checked at other stages of the process, as evidenced in the files provided, and that this issue relates solely to the input of pension increase runtime parameters.

2.3.8 Process

Pension Increases

Pension increases are tested either manually or via the PAS workflow based on a selection of Member records before they are finally applied. (see Control 2.2.8)

Control

An Administrator (Associate or above) carries out sample checks on the increases applied. These are checked by a Senior Administrator (Consultant or above) or another Administrator deemed competent by Management against the agreed increase level to confirm accuracy.

Once confirmed, either the Pensions Administrator or the Payroll Administrator finalise the workflow or sign off the Pension Increase checklist. Where a checklist is used it is retained on file or where a workflow is used, an audit trail is retained within the system as evidence of authorisation.

Auditor testing and results

For a sample of pension increases, confirmed an Administrator (Associate or above) carried out sample checks on the increases applied. Confirmed independent check by a Senior Administrator (Consultant or above) or another Administrator deemed competent by Management against the agreed increase level to confirm accuracy.

Inspected the workflow or sign off of the Pension Increase checklist to confirm this had been completed appropriately.

No exceptions noted.

2.3.9a Process

Pension Increases

A payroll file is prepared by an Administrator (Associate or above) and checked by a Senior Administrator (Consultant or above) or another Administrator deemed competent by Management. This is sent to the Client or payroll team to be applied to the Payroll database.

Control

The Administrator (Associate or above) prepares a file which is checked by a Senior Administrator (Consultant or above) or another Administrator deemed competent by management. The file is encrypted and sent across to the Client or payroll team for application to the payroll database.

Auditor testing and results

For a sample of pension increase calculations, confirmed these were reviewed by a Senior Administrator (Consultant or above) or another administrator deemed competent by Management. Confirmed the file was sent to the client or payroll team for application to the payroll database.

No exceptions noted..

2.3.9b Process

Profund only Pensions Increases

Once approved the Pension increases are applied to the PAS.

Control

The Pension increase calculations are approved by a Senior Administrator (Consultant or above) or another administrator deemed competent by Management and applied to the PAS. The increased pensions recorded on the PAS are applied through the appropriate pension payroll run through an automated process (see controls 2.3.5b and 2.3.6b).

Auditor testing and results

For a sample of pension increase calculations, confirmed these were approved by a Senior Administrator (Consultant or above) or another administrator deemed competent by Management and that this was applied to the PAS.

No exceptions noted.

2.3.10 Process

Pensions Increases

Where XPS Administration are contracted to send increase notifications they are prepared, checked and sent out in accordance with the Client agreement.

Control

Where required by the Client, the DB Administration team prepares the increase notifications. Increase letters are prepared by an Administrator (Associate or above) and checked by a Senior Administrator (Consultant or above) or another Administrator deemed competent by management.

The Payroll/ Administration Team check written notifications to ensure that all applicable members have been notified of the Pension Increase within the required timescale agreed with the Client and that members have been notified of the correct increases.

Auditor testing and results

For a sample of clients, confirmed the DB Administration team prepared the increase notifications. Inspected a sample of increase letters and confirmed these were prepared by an Administrator and checked by a Senior Administrator.

Confirmed notifications had been checked and that this had been completed within the required timescales agreed with the client.

No exceptions noted.

2.3.11a Process

Only authorised personnel can handle financially sensitive data with permissions set by the payment software.

Control

Access to authorise Payroll transmissions is restricted to individuals within the Payroll team. All transmissions are checked and authorised by a Senior Payroll Administrator (Consultant or above).

Payroll data which is sent externally for international payments is sent via a secure website.

Auditor testing and results

For a sample of transmissions, confirmed these had been checked and authorised by a Senior Payroll Administrator (Consultant or above). Through observation, confirmed Payroll data which is sent externally for international payments is sent via a secure website.

No exceptions noted.

2.3.11b Process

Profund only

Only authorised personnel can handle financially sensitive data with permissions set up in the PAS based upon role levels.

Control

Access to authorise Payroll transmissions is restricted to Senior Pension Administrators (Consultant or above) based upon role levels set up in the PAS.

Payroll data which is sent externally for international payments are sent via the normal payment process.

Auditor testing and results

For a sample of payroll transmissions, confirmed these had been approved by a Senior Pension Administrator.

No exceptions noted.

2.3.12a Process

Data transmission of financial data such as payroll uses secure encryption algorithms.

Control

BACS transmissions are encrypted. BACS transmissions may only be submitted once there has been approval by a Senior Payroll Administrator (Consultant or above) verifying the information that has been previously entered.

Auditor testing and results

Through observation confirmed that BACS transmissions may only be submitted once there has been approval by a Senior Payroll Administrator (Consultant or above) verifying the information that has been previously entered.

No exceptions noted.

2.3.12b Process

Profund only

Data transmission of financial data uses secure encryption algorithms.

Control

Bankline connections are encrypted by HTTPS. Bankline payments will only be released once there has been approval by at least one Senior Administrator (Consultant or above) verifying the information that has been previously entered. Depending on the payment amount most payments require 2 authorisations.

Auditor testing and results

Through observation, confirmed that the Bankline connection is encrypted by HTTPS.

No exceptions noted.

For release of payments through appropriate approval was tested under control 2.3.5c.

3. Maintaining financial and other records

3.1 Member records consist of up to date and accurate information

3.1.1-3.1.2 Process

For Clients with electronic data interfaces, Member data is kept up to date through periodic data loads including Payroll data and Human Resources information. The data loads are provided to XPS Administration by the Client in a pre-agreed format.

On receipt of a data file a Pensions Administrator follows the workflow steps to load the data onto the PAS. The PAS automatically produces error and warning reports and all errors are resolved prior to data being loaded. The data files and Interface Reports are retained centrally by the Administration Team, along with details of any enquiries arising from the data load and their resolution. Some Clients, Member data updates, including new joiners, leavers and DC investment options, are processed on a case by case basis. (see Control 3.1.6).

Control

3.1.1 On a monthly basis a DC Pensions Administrator reviews the PAS report which identifies unexpected differences or incorrect data between the Member data on the Client data file and PAS. Discrepancies are investigated, resolved and updated via the workflow. An audit trail of any amendments is maintained within PAS.

Auditor testing and results

For a sample of DC schemes, across a sample of months, confirmed a Pensions Administrator reviewed the PAS report of unexpected differences or incorrect data between the Member data on the Client data file and PAS.

Confirmed discrepancies were investigated, resolved and updated via the workflow.

No exceptions noted.

Control

3.1.2 A second DC Pensions Administrator verifies that any discrepancies identified on the errors and warnings report have been resolved. Once verified, the workflow is authorised electronically by the second Pensions Administrator. An audit trail is maintained within the PAS showing this authorisation. The reports are retained within the PAS.

Auditor testing and results

For the sample of DC schemes, across a sample of months in control 3.1.2, confirmed a second DC Pensions Administrator verified that discrepancies identified on the errors and warnings report have been resolved.

Inspected the workflow and confirmed authorised electronically by the second Pensions Administrator.

No exceptions noted.

3.1.3 Process

At least annually a Pensions Administrator reconciles the total number of Members in each of the Scheme Membership categories (e.g. active, deferred) to the previous report. This is done by running Membership reports from the PAS and taking into account any Membership movements in the period. The Membership reconciliation is included in the administration report presented to the client. (See section 5.2).

Control

At least annually a Pensions Administrator reconciles the Scheme Membership reports from the PAS back to the totals from the previous reconciliation, taking into account any Membership movements in the period. Any discrepancies are investigated and resolved. Once complete, a second Pensions Administrator reviews the reconciliation for accuracy. The Annual renewal or accounts checklist or workflow are completed and checked by independent administrators as evidence of the checks carried out.

Auditor testing and results

For a sample of schemes, inspected the Scheme Membership reports and noted that the Pensions Administrator had reconciled the reports from the PAS back to totals from the previous reconciliation and that any discrepancies had been investigated and resolved.

Confirmed that the corresponding checklist had been completed and signed as checked by an independent administrator.

No exceptions noted.

3.1.4 Process

On an annual basis the Pensions Administration Team complete an Annual Scheme Renewal. As part of this process, scheme contributions at Member level are validated where applicable, to ensure that they have been deducted and paid in accordance with the Scheme Rules.

Control

At least annually, the Pensions Administration Team validates salary and contributions data (where applicable) from the Client against historic data and correspondence to verify that the correct amounts have been paid on behalf the Member. Any inconsistencies are investigated and agreed with the Client. A copy of the Validation Report is saved electronically and any correspondence with the Employer is retained on the Scheme Renewal File.

A year end checklist or workflow is completed by an Administrator and signed off by a Senior Administrator (Consultant level or above) or another Administrator deemed competent by Management, to confirm the completion of the renewal.

Auditor testing and results

For a sample of schemes, confirmed that at least annually, the Pensions Administration Team validated salary and contributions data (where applicable) from the Client against historic data.

Confirmed inconsistencies were investigated and agreed with the Client.

Confirmed a copy of the Validation Report was saved electronically and any correspondence with the Employer is retained on the Scheme Renewal File.

Inspected the year end checklist or workflow and confirmed this was completed by an Administrator and signed off by a Senior Administrator (Consultant level or above) or another Administrator deemed competent by Management, to confirm the completion of the renewal.

No exceptions noted.

3.1.5 Process

The renewal process includes a reconciliation of the Scheme Membership and Member data against renewal data provided by the Client using membership reports generated from the PAS and taking into account Membership movements in the year.

Control

On an annual basis, a Pensions Administrator reconciles Membership totals on the PAS against renewal data provided by the Client. Any differences are investigated and resolved. The Annual Update Control Sheet or Workflow task is signed off by the Pensions Administrator and saved on the Scheme Renewal File. Reconciliation Reports and supporting documentation of any differences are retained electronically.

Auditor testing and results

For a sample of schemes, inspected the Annual Update Control Sheet Workflow task or checklist and Scheme Renewal File and noted that reconciliation of Membership totals to the PAS had been performed, including investigation and resolution of any differences and that the task or checklist had been signed off by the Pensions Administrator.

No exceptions noted.

3.1.6a Process

Personal Details Updates

Personal details are updated on receipt of e-mail, postal correspondence or telephone calls from Scheme Members or their suitably authorised representatives. All updates received by the Pensions Administration Team are updated onto the PAS and any details relating to pensioners are passed to payroll for update to the payroll system. All telephone calls from members and member pensioners are verified by checking at least two items of personal information, in order to verify their identity.

When notified of a member address change there is no requirement to complete the record of telephone call form. The address is changed on the system providing there is sufficient evidence in the communication to verify the member. A letter is sent to the old and new address to help combat fraud.

Control

A Pension/Payroll Administrator verifies the authenticity of member details prior to making changes to Member data. Verification of the authenticity of details is recorded on a record of telephone call form, letter or by completing a workflow. Where a workflow is used, an audit trail is retained in the PAS as evidence of authorisation. When notified of a change of address the Pensions Administrator will check to ensure that there is sufficient evidence to verify the member and change the address on the PAS. A letter is sent to both the old and new address. In the event of the address being changed in error the member has been made aware of the change and is asked to contact the department for verification. Any information in relation to the change is retained in the member file.

Auditor testing and results

For a sample of personal member detail updates, confirmed a Pension/Payroll Administrator verified the authenticity of member details prior to making changes to Member data through completion of the workflow/checklist.

For changes of address, confirmed the Pensions Administrator will check to ensure that there is sufficient evidence to verify the member and change the address on the PAS.

Confirmed letters were retained on file to evidence sending to old and new address to confirm the change.

No exceptions noted.

3.1.6b Process

Personal Details Updates

For the Middlesbrough and Bristol Cote House offices, personal details are updated on receipt of e-mail, postal correspondence or telephone calls from Scheme Members or their suitably authorised representatives. All updates received by the Pensions Administration Team are updated onto the PAS. Any details relating to pensioners are automatically updated into the payroll system. All telephone calls from members and member pensioners are verified by checking at least two items of personal information, in order to verify their identity.

When notified of a member address change there is no requirement to complete the record of telephone call form. The address is changed on the system providing there is sufficient evidence in the communication to verify the member. A letter is sent to the old and new address to help combat fraud.

Control

A Pension/Payroll Administrator verifies the authenticity of member details prior to making changes to Member data. Verification of the authenticity of details is recorded on a record of telephone call form, letter or by completing a workflow. Where a workflow is used, an audit trail is retained in the PAS as evidence of authorisation. When notified of a change of address the Pensions Administrator will check to ensure that there is sufficient evidence to verify the member and change the address on the PAS and will verify that the member's signature matches that held on file if the request is received in writing.

A letter is sent to the new address to confirm the change. In the event of the address being changed in error the member has been made aware of the change and is asked to contact the department for verification. Any information in relation to the change is retained in the member file.

Auditor testing and results

For a sample of personal member detail updates, confirmed a Pension/Payroll Administrator verified the authenticity of member details prior to making changes to Member data through completion of the workflow/checklist.

For changes of address, confirmed the Pensions Administrator will check to ensure that there is sufficient evidence to verify the member and change the address on the PAS and that the member's signature matched that held on file if the request is received in writing.

Confirmed a letter was retained on file to evidence sending to new address to confirm the change.

No exceptions noted.

3.1.7 Process

Member Investment Option Updates

Member investment options for new Members, or changes to existing Member's investment choices are updated either on receipt of an electronic Investment Instruction File from the Employer or on receipt of a written instruction from the Member. On receipt of an Investment Instruction File from the Employer the Administration Team prepare a data input file to update the Member records with investment choices or manually update the record. The Administration Team load the data input file to the PAS if required and update the Member records.

Control

Where electronic interfaces exist, the Administration Team performs sample checks against the data input file received from the Employer to verify the member's investment choices are updated accurately on the PAS. Once this is complete this is passed to a Senior Pensions Administrator (Consultant or above) or another Administrator deemed competent by management to spot check the inputs and sign off the workflow or control sheet as evidence of the review. This is retained on file.

Auditor testing and results

For a sample of changes to pension scheme member details and/or investment instructions, it was confirmed that changes were processed into PAS and independently validated by a Senior Pensions Administrator (Consultant or above) or another Administrator deemed competent by management

Confirmed that the workflow or control sheet had been completed to evidence review.

No exceptions noted.

3.1.8 Process

On receipt of a written instruction from the Member a Pensions Administrator sets up the investment instruction.

Control

On receipt of a written instruction from the Member a Pensions Administrator sets up the investment instruction.

A second Pensions Administrator verifies that details of the member record on the PAS match the written instruction and authorises the workflow as evidence of review.

Auditor testing and results

For a sample of investment instructions, it was confirmed that instructions were provided by the member (via system, email, letter) and set up by the Pensions Administrator. It was also confirmed that instructions were independently reviewed and authorised by a second Pensions Administrator.

No exceptions noted.

3.1.9a Process

New Pensioners and Dependants Updates

When setting up a new pensioner or dependant, a Pensions Administrator completes a New Pensioner/Dependant Form. The New Pensioner/Dependant Form is issued to the Payroll Team to create a Member record on the Pensioner Payroll. The new Pensioner/Dependant record on the Payroll Administration System is then verified to confirm it has been set up in accordance with the details recorded on the form.

Control

The workflow or New Pensioner/Dependant form is completed by an Administrator and checked by a second Administrator against the member details on the PAS and member benefit choices provided by the member. The amount of pension per annum dictates the seniority of the second person required to sign off the pension with increasing amounts of pension corresponding to increasing seniority of grade. The new Pensioner/Dependant form is signed off by the reviewer and sent to the Payroll team to set up on the Payroll Administration System.

Auditor testing and results

For a sample of new pensioners/dependants, confirmed the workflow or new pensioner/dependant form was prepared by an Administrator and checked by a second Administrator based on the appropriate seniority.

Confirmed the form was sent to the Payroll team for set up.

No exceptions noted.

3.1.9b Process

Non-Altair schemes

New Pensioners and Dependants Updates

When setting up a new pensioner or dependant, a Pensions Administrator creates a new record within the Altair system. The new Pensioner/Dependant record on the Altair system is verified to confirm it has been set up in accordance with the details recorded on the form.

Control

The New Pensioner/Dependant record is set up by an Administrator on the Altair database. Details are reviewed by a Senior Administrator (Consultant or above) against the member details on the PAS and member benefit choices provided by the member who approves payment of the pension.

Auditor testing and results

For a sample of new pensioners/new dependants, confirmed that the record had been set up by an Administrator and reviewed by a Senior Administrator. Confirmed that the benefit choices recorded on the PAS agreed to the member option forms and approval of the pension payment.

No exceptions noted.

3.1.9c Process

New Pensioners and Dependants Updates

When setting up a new pensioner or dependant, a Pension Administrator updates the PAS with the pension to be put into payment and sets the pension record to 'in payment' which ensures that the pension is put into payment.

Control

The member's pension record is updated by an Administrator with details of the pension to be put into payment and changed to 'in payment'. The record is checked by a second Administrator or Senior Consultant to ensure that the correct benefits have been put into payment.

Auditor testing and results

For a sample of member's pensions, confirmed the record was updated by an Administrator with details of the pension to be put into payment and changed to 'in payment'.

Confirmed the record was checked by a second Administrator or Senior Consultant to ensure that the correct benefits have been put into payment.

No exceptions noted.

3. Maintaining financial and other records

3.2 Requests to change member records are validated for authenticity

3.2.1 Process

XPS Administration are informed of a change to the Member's personal data by the Client's payroll or HR function or the Member directly. On a daily basis a Pension / Payroll Administrator creates a case in the Workflow system. For the processing of member personal updates, accuracy and completeness checks are performed against the source documentation (i.e. hard copy of Member data change request or scanned in equivalent) prior to completion of the workflow.

Control

A second Pensions/Payroll Administrator validates that all of the workflow steps and associated processes related to update of personal Member details have been performed correctly. The workflow or control sheet is authorised by the second administrator. Where a workflow is used, an audit trail is retained within the system as evidence of authorisation.

Auditor testing and results

For a sample of changes to member personal data, confirmed a second Pensions/Payroll Administrator validated that all of the workflow steps and associated processes related to update of personal Member details have been performed correctly.

Confirmed the workflow or control sheet was authorised by the second administrator.

No exceptions noted.

3. Maintaining financial and other records

3.3 Contributions and benefit payments are completely and accurately recorded in the proper period

3.3.1 Process

Payments are authorised by a second member of staff and released by an authorised signatory in accordance with the agreed controls. See controls in section 4.2.

Control

Payments are authorised by a second member of staff. See controls in section 4.2

Auditor testing and results

Please refer to control in section 4.2 which covers payment authorisations.

3.3.2 Process

Where CCM is not used, a payment request is raised by an Administrator using a Payment Request Form and authorised by a second individual. The form detailing the payment is added to the Client Banking System by a member of the Client Banking Team and approved in line with the controls in section 4.2.

Control

Where CCM is not used a payment request is raised by an Administrator using a Payment Request Form and authorised by a second individual. The form is approved in line with the controls in section 4.2.

Auditor testing and results

For a sample of payment requests, confirmed that a payment request form was completed by an Administrator and that this had been authorised by a second Administrator.

No exceptions noted.

3.3.3 Process

Bank reconciliations are performed at least monthly during which contributions and payments are checked for accuracy between bank statements and Client Banking records.

Each reconciliation includes:

- › a review of receipts received during the period of reconciliation
- › a review of payments made during the period of reconciliation
- › a forecast of expected payments and receipts in the coming reconciliation period
- › the expected balance at the end of the coming reconciliation period

Where discrepancies arise on the Client Banking system they are investigated and resolved with the Client Banking team and the Client if necessary.

Control

At least monthly, Scheme bank statements are reconciled against the Client Banking system, to verify that cash book entries have been accurately recorded in the Cash book. Any discrepancies are investigated and resolved.

The reconciliation is completed by a Client Banking Administrator (Associate or above) and authorised by a Client Banking team member senior to the Administrator. The reconciliation, along with correspondence relating to queries and their resolution, are retained by the Client Banking team.

Auditor testing and results

For a sample of schemes, and a sample of months, confirmed that the bank reconciliation was prepared by a Client Banking Administrator and subject to second review and approval by a Senior Administrator.

No exceptions noted.

3. Maintaining financial and other records

3.4 Investment transactions, balances and related income are completely and accurately recorded in the proper period

3.4.1 Process

Non-Profund

Timeliness and Accuracy of Complete DC Process

On a daily basis an Administrator checks the bank balance and electronic receipts. This ensures that all monies have been correctly recorded and paid out. On a monthly basis, the DC Team in each office obtains a ledger via CCM and reconciles it to the bank account.

Control

Daily downloads of receipts are updated by Client Banking into CCM and remain unallocated until a member of the DC Administration Team confirms how they should be allocated.

On a monthly basis all entries are reviewed by an Administrator (Associate or above) and checked by a Senior Administrator (Consultant or above), with any discrepancies investigated and resolved.

Where CCM is not used, depending on the frequency agreed with the client, the Accounts team receive the bank statements and upload into Aviary. The Senior Accountant then checks the bank statements to ensure all receipts have been picked up and allocated correctly.

Auditor testing and results

For a sample of schemes, and a sample of months, confirmed receipt allocations were reviewed as part of the bank reconciliation process by the Client Banking team. Entries are reviewed by an Administrator and checked by a Senior Administrator.

No exceptions noted.

3.4.2 Process

On a Monthly basis, the Administration Team extracts information from the PAS via an access database or using the PAS Control Accounts, to compare the unit holdings per Fund and per Scheme against the valuation of the holding obtained from the Investment Manager. Once completed this reconciliation is signed off by a Senior Administrator or above and updated on the DC Investment Tracker.

Investment transactions, balances and related income are posted to the nominal ledger by journals from investment Manager Reports. Investment cash is reconciled taking into account purchases, sales, investment income and charges; investment cost to cost and market value to market value reconciliations are performed as required for all Investment Managers; change in market value is reconciled to Investment Manager reports of realised and unrealised gains and losses.

Control

On a monthly basis, as part of the Contribution Process, unit holding information is extracted from the PAS via a securely linked access database or from Control Account information held within the PAS. The results of this are reconciled by the Administration Team against the Investment Manager Holdings with any differences identified being fully investigated, documented and if necessary ring-fenced until a cause for the difference is identified and can be resolved. Copies of any correspondence are retained on file as evidence. The Unit Reconciliation is reviewed by a Senior Administrator or above and a copy retained either on the file or electronically on the system. Completion and review of the Unit Reconciliation is reported in the monthly Managers Report where any issues are highlighted. The DC Investment Tracker is updated and reviewed at the Managers Meetings and documented on the Minutes to confirm review. See 6.2.1

Whilst it was confirmed that the Unit Reconciliation was performed, it was not evident, in all instances, that these had been reviewed by a Senior Administrator or above as this was not documented. As the control had not operated as described for the full reporting period, an exception is noted.

Exception noted.

Management response:

During 2021 we began the process of transferring many of our unit reconciliations to a central unit reconciliation team, with a small number continuing to be carried out by administration teams. Whilst building the central team and implementing the new reconciliation process we have noted there was unfortunately no formal process in place for unit reconciliations to be prepared and checked by two independent members of staff.

A formal checking process has been implemented with effect from September 2021 and RSM have noted that this process was working effectively after this date.

Completion of unit reconciliations is reported after this date to management on a monthly basis, with any issues flagged and management therefore have oversight of their completion.

We believe that this posed a low level of risk, as we have processes in place to ensure that any issues with unit reconciliations are resolved each month and that the reconciliations are reported to Management each month.

Auditor testing and results

For a sample of DC schemes, across a sample of months, confirmed that on a monthly basis, as part of the Contribution Process, that a unit holding reconciliation was performed by the Administration team. Confirmed differences identified were investigated and copies of correspondences were retained on file to evidence this.

3.4.3 Process

Investment transactions, balances and related income are posted to the nominal ledger by journals from investment Manager Reports. Investment cash is reconciled taking into account purchases, sales, investment income and charges; investment cost to cost and market value to market value reconciliations are performed as required for all Investment Managers; change in market value is reconciled to Investment Manager reports of realised and unrealised gains and losses.

Control

See 6.2.1

Auditor testing and results

Please refer to the testing in control 6.2.1

3. Maintaining financial and other records

3.5 Scheme documents are complete, up to date and securely held

3.5.1 Process

Original paper deeds, policies and contracts are on site by XPS Administration Limited

Control

Original paper deeds, policies and contracts are securely held by XPS Administration Limited. The documents are retained in a fireproof safe, which remains locked when not in use (see Control 7.1).

Auditor testing and results

Confirmed through observation that original paper deeds, policies and contracts are securely held in a fireproof safe, which remains locked when not in use.

No exceptions noted.

4. Safeguarding assets

4.1 Member records are securely held and access is restricted to authorised individuals

4.1.1 Process

Managing Data Protection

Responsibility for ensuring that the collection and use of data complies with Data Protection Law is allocated to all Business Managers. The Data Protection Manager provides advice and guidance on legislative requirements. All new staff receive data protection training when they join XPS Administration and refresher training is given annually. Staff sign a XPS Administration IT and Data Protection policy declaration, a copy of which is held on their HR record. Up to date information relating to the Data Protection Act and its application to XPS Administration are maintained on the XPS Administration Intranet, by the Data Protection Manager and is available to all staff.

See also controls 7.1, 7.2 and 7.9 for further details of the controls in place to protect data.

Control

All new staff are required to complete data protection training via an online platform when they join XPS Administration and refresher training is given annually.

On a monthly basis, completion of the data protection training is monitored by Compliance and reported back to the XPS Pensions Group Board for Board meetings at least quarterly.

Auditor testing and results

For a sample of new joiners, confirmed that data training had been completed.

For a sample of months, confirmed that the Compliance data provided reporting to the XPS Board on staff training to evidence ongoing monitoring of this.

No exceptions noted.

4. Safeguarding assets

4.2 Cash in scheme bank accounts is safeguarded and payments are suitably authorised

4.2.1a Process

A documented process is in place to maintain tiered mandates for release of payments, managed by the Client Banking Team. Authorisation levels are approved in writing by XPS Administration Management.

Addition and removal of staff from the mandates, and amendments to authorisation levels, is managed by the Client Banking Manager and retained by the Client Banking team. On receipt of approval the mandates are sent to the bank for implementation.

Control

The Client Banking Manager reviews the standard XPS Administration signatory list, and removes any company leavers and adds new members of the management team as required. The signatory list is authorised by Senior Management.

On receipt of approval the mandate is forwarded to the bank for implementation. Copies of the Trustee approval are retained on the scheme file.

Auditor testing and results

For the XPS Administration Signatory update made in the reporting period, confirmed the Client Banking Manager reviewed the standard XPS Administration signatory list, making updates as required. Confirmed the signatory list was authorised by Senior Management and inspected communication to the bank for implementation.

No exceptions noted.

4.2.1b Process

Altair only

Tiered mandates are used for the release of payments, managed by the Governance and Communications Manager. Authorisation levels are approved in writing by XPS Administration Management.

Control

The Governance and Communications Manager reviews the standard XPS Administration signatory list on an annual basis and removes any company leavers and adds new members of the management team. The signatory list is authorised by Senior Management.

Auditor testing and results

Confirmed the Governance and Communications Manager reviewed the standard XPS Administration signatory list at least on an annual basis. Confirmed the signatory list was authorised by Senior Management and distributed as required.

No exceptions noted.

4.2.1c Process

Profund only

Addition and removal of staff from the mandates, and amendments to authorisation levels, is managed and retained by the Governance and Communications Manager. On receipt of approval the mandates are sent to the bank for implementation.

Control

On receipt of approval the mandate is forwarded to the bank for implementation. Copies of the Trustee approval are retained on the scheme file.

Auditor testing and results

No testing was performed as there were no changes to the bank mandate during the period. Confirmed with management the control remains as described.

4.2.2 Process

Benefit payments (e.g. retirements, deaths, leavers) are prepared and reviewed by the Pensions Administration Team. See section 2.2 for details on benefit calculation.

Control

A Pensions Administrator verifies the payment details in the client communication against the payment details in the Pensions Administration System. The Control Sheet is signed off by a second Pensions Administrator and retained on file.

Auditor testing and results

For a sample of benefit payments, confirmed that the control sheet was prepared by one administrator and reviewed by another administrator.
No exceptions noted.

4.2.3a Process

The Pensions Administration Team prepares a standard client or member communication (depending on who the payment is made to) indicating the details of the payment, which is sent to the Pension Accounts Team for processing of payment. Payments are authorised and released in CCM or where CCM is not available by online banking or cheque.

Control

Payment details input to CCM are reviewed for accuracy and approved for release by two independent members of staff, according to authority levels established in a tiered mandate. All payments are authorised in line with the XPS signatory mandate and the Scheme bank mandate before being released.

Auditor testing and results

For a sample of CCM payments, confirmed these had been approved and released by two independent members of staff, according to established authority levels.

Confirmed payments were authorised in line with XPS signatory mandate and scheme bank mandate.

No exceptions noted.

4.2.3b Process

Altair Public Sector

The Pensions Administration Team prepares a standard client or member communication (depending on who the payment is made to) indicating the details of the payment, which is sent to the Pension Accounts Team for processing of payment.

Payments are authorised and released in the PAS.

Control

Payment details input to PAS are reviewed for accuracy and approved for release by one member of the Management team and by the Client, according to authority levels established in a tiered mandate.

All payments are authorised in line with the Middlesbrough office signatory mandate and the Scheme bank mandate before being released.

Auditor testing and results

For a sample of benefit payments it was confirmed that the payment request form was appropriately prepared by an Administrator or above, and reviewed by a Senior Administrator or above. It was confirmed that client authorisation was obtained prior to the payment being processed. Confirmed payments were processed after all approvals had been submitted.

No exceptions noted.

4.2.3c Process

Altair non-Public Sector

The Pensions Administration Team prepares a standard client or member communication (depending on who the payment is made to) indicating the details of the payment, which is sent to the Pension Accounts Team for processing of payment. Payments are authorised and released in CCM or where CCM is not available by online banking or cheque.

Control

DC Schemes: Payment details input to CCM are reviewed for accuracy and approved for release by two independent members of staff, according to authority levels established in a tiered mandate. All payments are authorised in line with the XPS signatory mandate and the Scheme bank mandate before being released.

DB schemes: Payment details input to CCM are reviewed for accuracy and approved for release by an independent member of staff through the workflow system, according to authority levels established in a tiered mandate. The payroll team review the details input and arrange for payment to be made.

Effective up to 30 September 2021

Auditor testing and results

For a sample of payments, confirmed these had been approved for release by two independent members of staff. DC Schemes: Payment details input to CCM are reviewed for accuracy and approved for release by two independent members of staff, according to authority levels established in a tiered mandate. All payments are authorised in line with the XPS signatory mandate and the Scheme bank mandate before being released.

No exceptions noted.

4.2.3d Process

Profund only

The Pensions Administration Team prepares a standard client or member communication (depending on who the payment is made to) indicating the details of the payment, which is sent to the Pension Accounts Team for processing of payment.

A payment request form is set up and completed by an Administrator and reviewed by a Senior Administrator before being input and reviewed in the Bankline system by an Administrator and Senior Administrator.

The payment is then authorised in the Bankline system, according to the authority levels established in the tiered mandate.

Control

For both DC and DB Schemes: A payment request form is completed by an Administrator (Associate or above) and reviewed by a Senior Administrator (Consultant or above) before being input into the CCM/Bankline system.

Payment details input to Bankline are reviewed for accuracy and approved for release by two independent members of staff, according to authority levels established in a tiered mandate. For CCM payments, these are reviewed for accuracy and approved for release by one member of the team and then follows to Cashiering. All payments are authorised in line with the XPS signatory mandate and the Scheme bank mandate before being released.

Auditor testing and results

For a sample of payments, obtained the payment request form and confirmed this had been completed by an Administrator (Associate or above) and reviewed by a Senior Administrator (Consultant or above) before being input into the CCM/Bankline system. Inspected payment detail form input to Bankline were reviewed for accuracy and approved for release by two independent members of staff, according to authority levels established in a tiered mandate. For CCM payments, confirmed these had been approved for release by one member of the team and then follows to Cashiering team.

No exceptions noted.

4.2.4a Process

Electronic payment files are imported by CashFac managed services for payment on the Bank's Electronic Payment System. Once payments are uploaded, the payment is authorised by a Client Banking staff member.

Control

Access to release and approve payments in the relevant Bank's electronic payment system is restricted to authorised Client Banking Administrators via the use of individual access cards and unique PIN.

Auditor testing and results

Through observation confirmed access to release and approve payments in the relevant Bank's electronic payment system is restricted to authorised Client Banking Administrators via the use of individual access cards and unique PIN.

No exceptions noted.

4.2.4b Process

Altair Schemes

Electronic payment files are imported by CashFac managed services for payment on the Bank's Electronic Payment System. Once payments are uploaded, the payment is authorised by a Client Banking staff member.

Control

Access to release and approve payments in the relevant Bank's electronic payment system is restricted to authorised Accounts Administrators via the use of individual user name and password.

Auditor testing and results

Through observation confirmed access to release and approve payments in the relevant Bank's electronic payment system was restricted to authorised Accounts Administrators via the use of individual user name and password.

No exceptions noted.

4.2.4c Process

Profund Schemes

Electronic payment files are imported by CashFac managed services for payment on the Bank's Electronic Payment System. Once payments are uploaded, the payment is authorised by a Client Banking staff member.

Control

Access to release and approve payments in the relevant Bank's electronic payment system is restricted to authorised Accounts Administrators via the use of individual username and password.

Auditor testing and results

Through observation confirmed access to release and approve payments in the relevant Bank's electronic payment system is restricted to authorised Accounts Administrators via the use of individual username and password.

No exceptions noted.

4.2.5 Process

Cheque Payments

Where cheque payments are required, they are approved by a second Pension Administrator on the CCM or using a Payment Request form. 2 authorised signatories from the client bank mandate are required to sign the cheque as per the client bank mandate.

Where agreed with the client, pre-approved cheques are used which are authorised by two Client signatories. Payments are approved by a second Pension Administrator on the CCM or using a Payment Request form.

Control

Cheque Payments are approved by a second Pension Administrator via the CCM system or using a Payment Request form. The cheque is signed by two authorised members of staff as per the client bank mandate.

Where pre-approved cheques are used these are securely retained in a pin code safe.

Auditor testing and results

For a sample of cheque Payments, confirmed these had been approved by a second Pension Administrator via the CCM system or using a Payment Request form. Inspected the corresponding cheque and confirmed this had been signed by two authorised members of staff.

Via observation, confirmed that where pre-approved cheques are used, that these were securely retained in a pin code safe.

No exceptions noted.

4.2.6a Process

Payment Receipts

Cheques are logged upon receipt and banked promptly by a member of the Client Banking team unless subject to a query. The Administration team provide backing paperwork confirming details of the payment received.

Control

Receipts are allocated by the Client Banking team based upon information provided by the Administration team through the CCM or by e-mail. Any queries regarding the receipt are raised with the Client or other Third Party prior to the payment being banked.

Auditor testing and results

For a sample of receipts, confirmed these had been allocated by the Client Banking team. Inspected the supporting evidence to confirm allocation matched the receipt. For the sample tested, no queries regarding the receipt were raised with the Client or other Third Party prior to the payment being banked. Enquired with management who confirmed the control remains as described.

No exceptions noted.

4.2.7 Process

Scheme expenses are submitted to the Client Banking Team for settlement upon receipt. The expense invoice is authorised by the Scheme Trustees and submitted to the Client Banking team by the Administration team either through the PAS or by e-mail.

Control

Where expenses are being submitted payment instructions are approved by a second member of staff and released by an authorised signatory in accordance with the bank mandate. The Cashiering team checks against client specific limits and authorised signatories shown on customised forms.

Payment of expenses is approved only if the payment form is authorised by a scheme officer or trustee or is within specific agreed signing requirements for the relevant scheme.

Auditor testing and results

For a sample of scheme expenses, confirmed payment instructions are approved by a second member of staff and released by an authorised signatory in accordance with the bank mandate. Confirmed payment of expenses was approved only if the payment form was authorised by a scheme officer or trustee or is within specific agreed signing requirements for the relevant scheme.

No exceptions noted.

5. Managing and monitoring compliance and outsourcing

5.1 Receipt of contributions are monitored against required timescales

5.1.1 Process

The DC Administration Team monitor the receipt of contributions and associated contribution data against agreed dates recorded on an Investment Tracker. Where contributions and contribution data has not been received by the agreed date, the DC Administration Team contacts the Client to arrange for them to be sent to the Scheme bank account. A copy of this correspondence is held on the Monthly Investment File.

Control

On a monthly basis the DC Administration Team or the Client Banking Team monitor receipt of contributions and associated contribution data against agreed dates on the Investment Tracker to ensure that these are received before the 22nd of the next month as required by The Pensions Regulator.

Where contributions and contribution data have not been received by the agreed date, the DC Administration Team contacts the Client to arrange for them to be sent to the Scheme bank account.

Auditor testing and results

For a sample of months, for a sample of schemes, confirmed the DC Administration Team or Client Banking Team recorded the monitoring of receipt contributions on the Investment Tracker to ensure these are received as required by The Pensions Regulator.

Where these had not been received by the agreed date, inspected emails to evidence the DC Administration Team following up with the client to arrange for these to be sent.

No exceptions noted.

5.1.2 Process

The DC Administration Team update the Investment tracker spreadsheet with progress of the monthly investment process. Any contributions which are invested outside of the SLA are reported to the Client and a loss assessment is completed.

Control

Progress of monthly investments for all DC Clients is monitored by the DC Administration Team on a monthly basis using the Investment Tracker, diarised reminders or via the workflow system. Any investments that fail to meet the Client's SLA are reported immediately to the Client. The DC Administration Team prepares and sends a loss assessment to the Client, where requested by the Client. A Monthly Report is presented at the Manager's meeting at least quarterly as evidence that investments have been made within the timescales agreed in the SLA.

Auditor testing and results

For a sample of months, confirmed progress of monthly investments for all DC Clients was monitored by the DC Administration Team monthly through the Investment Tracker, diarised reminders or via the Workflow system.

For the sample inspected, no investments failed to meet the client's SLA, therefore, no further testing was conducted. Management confirmed the control remains as described.

Obtained monthly report and confirmed this was presented at least quarterly at the manager's meeting.

No exceptions noted.

5.1.3 Process

Receipt of DB Contributions

The Client is responsible for ensuring that the DB Contributions are paid into the Trustees Bank Account in line with the Schedule of Contributions or at the latest, for contributions deducted from members pay, by 22nd of each month if paid electronically (19th of month if paid manually).

Control

On a monthly basis, the Client Banking or administration team uses a tracking document or diarised reminders to monitor receipt of contributions. Any missing contributions are pursued with the Client and if payment is not forthcoming escalated to Senior Management for consideration of reporting under The Pensions Regulator Whistleblowing guidelines.

Auditor testing and results

For a sample of schemes across a sample of months, inspected the tracking documented used by the Client Banking or administration team to monitor receipt of contributions. For the sample tested, there were no missing contributions and confirmed with management that the control remains as described.

No exceptions noted.

5. Managing and monitoring compliance and outsourcing

5.2 Pensions administration activities are governed by service level agreements that are authorised and subject to regular review. Service performance is regularly monitored and assessed against standards set out in service level agreement

5.2.1 Process

All work received in the Pensions Administration Department is logged into the workflow system. The system automatically allocates a Service Level Agreement (SLA) date based on the case type created. The Administration system tracks each case against SLA elapsed time. Management Information comparing actual case processing performance against SLA targets is produced on a monthly basis.

Control

The Business Services Group (BSG) produce a Monthly Management Report confirming performance against client Service Level Agreements which is sent to XPS Management. The report is discussed at either formal or informal meetings at least quarterly, with actions taken to resolve any issues raised.

Auditor testing and results

For a sample of months, confirmed that a monthly management report was produced by BSG and sent to XPS management. Confirmed the reports contained KPIs and SLA across sites/ schemes. Inspected quarterly agenda to confirm BSG report discussed.

No exceptions noted.

5.2.2 Process

The Pensions Administration Team produce a formalised annual plan for each scheme detailing the tasks which need to be completed throughout the year. This is used to manage the timing of periodic and annual transactions.

Control

The Pensions Administration team produce an annual plan/ Alfresco task list to manage and monitor periodic and annual transactions, scheme level and non-member related activities. The plan is held electronically on the system and reviewed and updated by the Team Leader or Manager annually.

Auditor testing and results

For a sample of schemes, confirmed that an annual plan/ Alfresco task list to manage and monitor periodic and annual transactions, scheme level and non-member related activities was in place. Confirmed the plan is held electronically on the system and reviewed and updated by the Team Leader or Manager annually. No exception noted.

No exceptions noted.

5. Managing and monitoring compliance and outsourcing

5.3 Transaction errors are identified, reported to clients and resolved in accordance with established policies

5.3.1 Process

When a complaint is received it is logged into a central Complaint Management System by an Administrator (Associate or above) and reported to the client.

Key information relating to the complaint is recorded in the Complaint Management System which is used to track the progress of the complaint through to resolution and monitor that responses are issued in a timely fashion. Each complaint is thoroughly investigated by a member of the Pensions Administration Team, in accordance with the XPS Administration Complaint handling procedure. When the complaint is completed, the record is closed in the Complaint Management System as confirmation that the complaint has been thoroughly investigated and resolved within the specified SLAs.

Control

Complaint related correspondence is reviewed by a Pensions Administration Team Leader or above and agreed with the client where requested by the client themselves. Details of the complaint are captured on the Complaint Management System and reviewed to verify that all complaint details are captured, investigated and resolved within the SLA set down between XPS Administration and the Client and within FCA defined timescales if applicable. Where the case is not dealt with by a Team Leader, correspondence is signed off by the Team Leader prior to issuance. Copies of signed off correspondence are retained on the Scheme or Member file. All complaints are reported to clients in their next administration report following the complaint being logged.

Auditor testing and results

For a sample of complaints, confirmed correspondence was reviewed by a Pensions Administration Team Leader or above and agreed with the client where requested by the client themselves.

Confirmed details of the complaint were captured in the Complaint Management System and that these were reviewed.

Confirmed complaints reported in the next Admin report to the client following the complaint being logged.

No exceptions noted.

5.3.2 Process

When a transaction or calculation error is identified, Root Cause Analysis is undertaken, including action taken to ensure that the error doesn't occur again. Where a financial loss is identified details of the Root Cause Analysis are recorded in the Complaint Management System, and where compensation is paid, on a compensation payment request form.

Control

Compensation claims details and Root Cause Analysis are reviewed by the Pensions Administration Manager/Team Leader to verify that corrective action has been taken to prevent a repeat of the error. Claim details including calculation of claim amount are verified for accuracy. Once complete, and where necessary, the Pensions Administration Manager/Team Leader completes the Root Cause Analysis fields in the Complaint Management System and completes and signs off the compensation payment request form.

Auditor testing and results

For a sample of compensation claims, confirmed the Root Cause Analysis was completed and reviewed by the Pensions Administration Manager/Team Leader.

Once the review had been completed, confirmed fields had been completed and the corresponding compensation payment request form had been signed off by the Pensions Administration Manager/Team Leader.

No exceptions noted.

5.3.3 Process

The compensation payment request form is signed off in line with compensation limits and sent to the Finance Team to arrange for payment.

Control

All compensation Payment request forms are signed off in line with limits outlined in Complaints Handling guidance prior to an agreement to pay compensation.

Auditor testing and results

For a sample of compensation payments, confirmed the request forms were signed off in line with limits outlined in Complaints Handling guidance prior to an agreement to pay compensation.

No exceptions noted.

5. Managing and monitoring compliance and outsourcing

5.4 Periodic reports to The Pensions Regulator and HMRC are complete and accurate

5.4.1 Process

The XPS Administration TPR breaches guidance includes guidance on regulatory breaches, including when a regulatory report is required, and how the report should be made.

Control

When a regulatory breach is identified a report is prepared by a designated person (i.e. Administration Manager/Team Leader, Consultant or Actuary) and submitted to the Client Principal or Client as per the agreed process for the scheme. The Client Principal or Client reviews the report and identifies the level of the breach.

The regulatory breach log is then updated with details of the breach and the decision made.

Where the Client Principal or Client decides that the breach needs to be reported to the Pensions Regulator, the report is then submitted to the regulatory body and a copy retained on file.

Auditor testing and results

For a sample of breaches, confirmed these had been reported by a designated person and submitted to the Client Principal or Client. Confirmed that a level of breach was assigned and that the regulatory breach log was updated with the details and decision made. For the sample of breaches reviewed, none were reported to the Pensions Regulator. Upon enquiry with management it was confirmed that where a report is submitted, the control operates as described.

No exceptions noted.

5.4.2 Process

The Pensions Regulator Scheme Return is completed by the Pensions Administration Team where requested by the Client.

Control

On an annual basis, where agreed with the client a Pensions Administrator completes the annual Pensions Regulator Scheme Return. This is reviewed by an independent Pensions Administrator or the Client, as agreed with the Client.

Auditor testing and results

For a sample of schemes, confirmed that the annual Pensions Regulator Scheme Return was prepared by an Administrator. Confirmed this is reviewed by an independent Pensions Administrator or the Client, as agreed with the Client.

No exceptions noted.

5.4.3 Process

Data Breaches are reported by a Senior Administrator (Consultant level or above) or another Administrator deemed competent by Management to the Compliance team.

Control

Upon identification of a potential data breach, the Administration Team notifies the XPS Group Compliance team that a breach has occurred via an online breach form. The Compliance team will log the potential breach onto the GDPR breach log.

The Compliance team review the facts, requesting additional information if required, and advise the Senior Administrator on whether a breach has occurred and the next steps to be taken.

Where advised by Compliance the Administration team will prepare a communication to the Data Controller (Client).

Auditor testing and results

For a sample of breaches confirmed these had been reported via the breach form and logged as received by a member of the Compliance team. Confirmed communication was issued to the client where advised by Compliance.

No exceptions noted.

5.4.4 Process

Breaches are monitored centrally by the Compliance team. Quarterly reports are provided to senior management on the number of breaches received.

Control

Data breaches are monitored centrally by the Compliance team. Quarterly reports are provided to senior management on the number of breaches received and breach trends.

Auditor testing and results

For a sample of months, confirmed that the compliance report was produced and that this was issued to senior management through discussion at the corresponding Board meetings. Inspected the report and confirmed contains breaches raised and trends.

No exceptions noted.

5.4.5a Process

Subject Access requests are responded to in accordance with the General Data Protection Regulations (GDPR).

Subject Access requests are monitored centrally by the Compliance team. Periodic reports are provided to senior management on the number of subject access requests received.

Control

On receipt of a potential Subject Access Request the Administration team log the request via a sharepoint form with the XPS Compliance team who assess whether a valid Subject Access request has been received. The Data Controller is advised that a valid SAR has been received and an acknowledgement is sent to the requester.

The Administration team collate the data held on the Data Subject. The collated information is passed to the Compliance team to review. The Data Protection Manager or another member of the Compliance team reviews and signs off the file to be sent.

The Administration team sends the file securely to the Data Controller, or directly to the Data Subject (as agreed with the client) within the one month timeframe specified under GDPR.

If there is going to be any delay in providing the information to the Data Subject a letter informing them of the delay is sent in line with the guidelines set out in the GDPR.

Auditor testing and results

For a sample of SAR requests, confirmed these had been assessed as valid requests. Confirmed that the data controller had been informed of the request. Confirmed that the DPM/Compliance had approved the SAR release and that this had been sent within the one month deadline stated by GDPR.

No exceptions noted.

5.4.5b Process

Altair schemes only

Subject Access requests are responded to in accordance with the General Data Protection Regulations (GDPR).

Subject Access requests are monitored centrally by the Pensions Administration team through the Middlesbrough SAR Log and sent to the DP Manager on a monthly basis.

Control

On receipt of a potential Subject Access Request the administration team log the request and confirm with the Data Controller whether a valid Subject Access request has been received.

The administration team collate the data held on the Data Subject, and sends the file securely to the Data Controller to transmit to the Data Subject, within the one month timeframe specified under GDPR.

If there is going to be any delay in providing the information to the Data Subject a letter informing them of the delay is sent in line with the guidelines set out in the GDPR.

Auditor testing and results

For a sample of requests it was confirmed that XPS received a SARS request from the data subject, it was confirmed that the Admin team obtained consent and approval from the Data Controller, prior to issuing and confirming SARS completion to the Data Controller, within the one month timeframe.

No exceptions noted.

6. Reporting to clients

6.1 Periodic reports to participants and scheme trustees are complete, accurate, and provided within required timescale

6.1.1 Process

A timetable for reporting is agreed with the Client and includes regular (usually quarterly or half yearly) Administration Reports as agreed. Reports are prepared by the Pensions Administration Team and reviewed by a Senior Administrator (Consultant or above) or another Administrator deemed competent by management before being issued to the Client.

Control

At a frequency agreed with the Client, Administration Reports are prepared by a Pensions Administrator and reviewed for accuracy and completeness by a Senior Administrator (Consultant or above) or another Administrator deemed competent by Management.

The report is submitted to the Client with a copy of the report retained on file.

A workflow is signed off as evidence of the completion of the Administration report.

Auditor testing and results

For a sample of schemes, confirmed that a Admin report was prepared by an Administrator and that this was reviewed by a Second Administrator. Obtained a copy of the report and confirmed these were retained on file. Where applicable, confirmed that the workflow was signed off as complete.

No exceptions noted.

6.1.2 Process

The Annual Benefit Statement exercise is managed by the Administration Team. The Benefit statement checklist is used as guidance for the process to be followed and to ensure that statutory and Client deadlines are met.

As part of the process, a statistically representative sample of calculations is verified to confirm accuracy.

A Benefit Statement template is agreed with the client. Once calculations have been agreed, the Administration team populate the template with the calculation results. The completed templates are independently checked to confirm that they are accurate and match calculation results.

Control

On an annual basis, an Administrator (Associate or above) carries out Benefit Statement calculations using the Benefit Statement checklist and any scheme specific guidance. A statistically representative sample of Benefit Statement calculations are reviewed by a Senior Administrator (Consultant level or above) or another Administrator deemed competent by Management, to ensure that these have been carried out correctly.

Once calculations have been checked the Benefit statement template is populated by an Administrator with the calculation results and checked by the Senior Administrator (Consultant or above) or another Administrator deemed competent by Management.

Once the process has been completed, the Benefit Statement Checklist or workflow is signed as evidence of review by a Senior Administrator (Consultant or above) or another Administrator deemed competent by Management.

Auditor testing and results

For a sample of schemes, confirmed that the annual benefit statement calculations had been prepared and subject to review by an independent person. Confirmed that the checklist/workflow had been completed.

No exceptions noted.

6.1.2b Process

The Annual Benefit Statement exercise is undertaken via an automated process through the PAS. This process is managed by the Governance and Comms manager with input from BSG and ASG. The Benefit statement checklist is used as guidance for the process to be followed and to ensure that statutory and Client deadlines are met.

As part of the process, a statistically representative sample of calculations is verified to confirm accuracy.

Once the results have been agreed they are automatically loaded to the member web platform.

Control

On an annual basis, Benefit Statement calculations are carried out through an automated process in the PAS. The Benefit statement checklist is used as guidance for the process to be followed and to ensure that statutory and Client deadlines are met.

This process is managed by the Governance and Communications manager with input from BSG and ASG.

Auditor testing and results

For a sample of schemes confirmed that the Benefit Calculations we performed through the PAS. Confirmed that these had been performed within the statutory deadline. Confirmed evidence was provided to demonstrate that the process is managed and overseen by the Governance Manager.

No exceptions noted.

6. Reporting to clients

6.2 Annual reports and accounts prepared for pension schemes are completed, accurate and provided within required timescales

6.2.1 Process

Production of the annual Trustee Report & Accounts is scheduled in the Scheme timetable. A Scheme Year End Accounts Checklist is used as a guide to the completion of the Annual Scheme Accounts. The Year End Accounts process includes the following:

- › All cash payments/receipts from the Trustee administration bank account are reconciled to cash receipts/payments reported by the Investment Managers;
- › Investment transactions, balances and related income are posted to the nominal ledger by journals from Investment Manager reports;
- › Investment cash is reconciled taking into account purchases, sales, investment income and charges;
- › Investment cost to cost and market value to market value reconciliations are performed as required for all Investment Managers;
- › Change in market value is reconciled to Investment Manager reports of realised and unrealised gains and losses.

Control

On an annual basis, the Pension Accountant reviews the draft accounts to verify the accuracy and completeness of the content, figures and disclosures. All statements are reviewed against the model example statements contained in the Statement of Recommended Practice (SORP), and the content is reviewed for legislative and regulatory guideline changes. Once satisfied, the Pension Accountant signs off the Scheme Year End Accounts Checklist as evidence of review. The draft accounts are reviewed and the Scheme Year End Accounts Checklist signed off by a second Pension Accountant or a Senior Manager.

Auditor testing and results

For a sample of schemes for whom XPS prepared accounts, confirmed the Pension Accountant reviewed the draft accounts to verify the accuracy and completeness of the content, figures and disclosures.

Inspected the Scheme Year End Accounts Checklist and confirmed the Pension Accountant signed off as evidence of review.

Confirmed the draft accounts were reviewed and the Scheme Year End Accounts Checklist was signed off by a second Pension Accountant or a Senior Manager.

No exceptions noted.

6.2.2 Process

Annual report and accounts are prepared in compliance with the latest Statement of Recommended Practice (SORP) for pension schemes based on a standard report format.

Control

The accountant updates the standard reporting format to take into account any changes in legislation. Annual accounts are prepared and then checked by a Senior Accounts Administrator (Consultant or above) or another Accounts Administrator deemed competent by Management prior to audit. Audited accounts, once approved, are signed off by the Trustees.

Auditor testing and results

For a sample of schemes, confirmed the accountant updated the standard reporting format to take into account any changes in legislation. Confirmed annual accounts were prepared and then checked by a Senior Accounts Administrator (Consultant or above) or another Accounts Administrator deemed competent by Management prior to audit. Confirmed Audited accounts, once approved, were signed off by the Trustees.

No exceptions noted.

6.2.3 Process

Progress of production of Scheme Accounts is monitored against agreed and statutory deadlines.

On a monthly basis or as agreed with the Client, the Management team are provided with management information progress for the Individual Schemes, production of accounts, including any potential breaches of the Pensions Act 1995 seven month deadline.

Control

At least monthly the Pensions Accounts Team Leader reviews the completion of Annual Accounts against the Accounts Production Schedule. The schedule is updated with progress and any concerns are discussed with the Pension Accountant. A copy of the schedule is retained in Pension Accounts.

Auditor testing and results

For a sample of months, confirmed the Pensions Accounts Team Leader reviewed the completion of Annual Accounts against the Accounts Production Schedule. Confirmed a copy of the schedule was retained in Pension Accounts.

No exceptions noted.

7. Restricting access to systems and data

7.1 Physical access to in-scope systems is restricted to authorised individuals

7.1.1-7.1.2 Process

Entry to XPS offices is restricted to authorised personnel and visitors. All offices have a card or fob access system to the office area and visitors are required to sign in at reception and are collected and escorted from reception. There are 13 offices in scope for this report as follows:

Belfast	Reading	Newcastle	Wokingham	Birmingham	Middlesbrough
Perth	Edinburgh	Bristol	Bristol – Cote House	Chelmsford	Leeds London

Control

7.1.1 Entry to floors occupied by XPS is controlled by a card, fob or key access system. Visitors are required to sign in at reception and are collected and escorted from the reception area.

Auditor testing and results

For a sample of office locations, inspected evidence of physical access controls. Noted that entry to floors was restricted by either card, fob or key access, and visitors were required to sign-in at reception and be collected by an escort. **No exceptions noted.**

Control

7.1.2 Access cards, fobs, office keys are issued upon receipt of a new starter notification from a Manager of the business or recruitment administrator.

Auditor testing and results

For a sample of offices, inspected request documentation for the issue of access cards, fobs, and office keys. Noted that office access was provisioned upon receipt of a request and approval from a Manager or recruitment administrator. **No exceptions noted.**

7.1.3 Process

Physical access to the areas containing the IT infrastructure is restricted with access gained by swipe card access, keypad access or lock and key. Any access request for any individual is granted by XPS IT Management.

The sites with areas containing IT infrastructure are:

Reading Belfast Leeds Edinburgh Middlesbrough Wokingham

Control

Access to the IT processing facilities (Comms Rooms) is restricted by swipe card access, keypad access or lock and key. Access is restricted to IT staff, or staff who have been given authorisation from XPS IT Management or Office Management.

Auditor testing and results

For a sample of offices, inspected access restrictions and request documentation for access to IT processing facilities. Noted that IT processing facilities access was physically restricted to appropriate personnel, and access requests provisioned with approval.

No exceptions noted.

7.1.4 Process

The sites with areas containing Comms Rooms are as follows:

Reading Belfast Leeds Edinburgh Middlesbrough Wokingham

Where offices have Comms Rooms these contain the local IT infrastructure and are air conditioned and monitored and alerted for:

- › Temperature
- › Fire
- › Water Detection
- › Fire extinguishers are available inside or near to the room. An Uninterruptible Power Supply (UPS) is deployed in the event of a mains outage or power spike.

Control

Where offices have Comms rooms, they are equipped with environmental protection controls including:

- › Automated fire detection mechanisms
- › Fire extinguishers
- › Air conditioning
- › UPS

Auditor testing and results

For a sample of offices, inspected evidence that the IT processing facilities contained appropriate environmental controls, including fire detection/suppression, UPS, and air conditioning. Noted that these facilities were equipped with environmental protection controls.

No exceptions noted.

7. Restricting access to systems and data

7.2 Logical access to in-Scope systems and data is restricted to authorised individuals in accordance with job roles and/or business requirements

7.2.1 Process

Network Operating System: Identification and Authentication

Logical access to network resources, by users and IT Services is controlled via unique user logons and self-select passwords which must conform to industry standard length and complexity rules. Passwords expire after a set number of days and history prevents re-use.

Control

Identification and Authentication
User accounts are identified to the network through unique user ID's and passwords

Auditor testing and results

Inspected the group policy password configuration for the domains and noted that password setting requirements were configured in line with industry standards. Inspected system and domain account populations and noted that users gained access through a unique user ID.

No exceptions noted.

7.2.2 Process (non-Altair)

Network Operating System: Lockouts

User accounts are locked out after a set number of failed attempts to authenticate. The user must raise a ticket with IT Services to unlock the account. The user will be asked to identify themselves using a unique identifier. IT Services can provide metrics on the number of user accounts they have unlocked to the XPS IT Management if required.

Control

User accounts and administrator accounts are locked out after three failed attempts. Accounts are unlocked by IT Services upon receipt of a ticket which is logged by the user. Logged requests are retained and the information is provided to the XPS IT Management on request.

Auditor testing and results

Inspected the domain account lockout configuration and noted that all accounts are locked out after three failed attempts.

For a sample of lockout requests, inspected the service desk ticket raised and noted that accounts were unlocked by IT services upon receipt of a ticket logged by the user, with the request retained.

No exceptions noted.

7.2.3a-7.2.3g Process

Application: Identification and Authentication

Logical access to the schemes administration application by Pensions Administrators is controlled via unique user login and self-select passwords or through Windows user accounts. Passwords expire after a set number of days and password history prevents re-use within a set number of valid changes as per XPS IT password rules.

Control

7.2.3a Compendia

Users are identified to the scheme administration application through unique user IDs and passwords. Accounts are set up following approval from Line Managers via the BSG Helpdesk systems which are retained in the system for review.

7.2.3b Penscope

Users are identified to the scheme administration application through unique user IDs and passwords. Accounts are set up following approval from Line Managers via the XPS IT and/or BSG Helpdesk systems which are retained in the system for review.

7.2.3c Alfresco

Users are identified to the scheme administration application through unique user IDs and passwords. Accounts are set up following approval from Line Managers via the XPS IT Helpdesk systems which are retained in the system for review.

7.2.3d Resource Link

Users are identified to the scheme administration application through unique user IDs and passwords. Accounts are set up following approval from a Payroll Team Leader via the BSG Helpdesk systems which are retained in the system for review.

7.2.3e Altair

Users are identified to the scheme administration application through unique user IDs and passwords. Accounts are set up following approval from Line Managers via the XPS IT Helpdesk system. These have a specific profile attached which determines actions that users can undertake (scheme access, processes, reports, etc.)

7.2.3f Profund Classic

Users are identified to the scheme administration application through unique user IDs and passwords. Accounts are set up following approval from Line Managers via the XPS IT Helpdesk system or by request to the Pension Systems Manager which are retained in the system for review.

7.2.3g Profund oPEN2

Users are identified to the scheme administration application through AD user IDs and passwords. Accounts are set up following approval from Line Managers via the XPS IT Helpdesk systems.

These have a specific profile attached which determines actions that users can undertake (scheme access, processes, reports, etc.).

Auditor testing and results

For a sample of accounts created across the in-scope systems, inspected the ticket raised for systems access and the associated approval. Noted that all requests received appropriate approval.

No exceptions noted.

Control

7.2.4a Compendia

The schemes administration application passwords are configured by BSG and require a combination of alphanumeric characters and a pre-defined password length.

7.2.4b Penscope

The schemes administration application passwords are defined at an AD level and configured by XPS IT and require a combination of alphanumeric characters and a pre-defined password length.

7.2.4c Alfresco

The schemes administration application passwords are defined at an AD level and configured by XPS IT and require a combination of alphanumeric characters and a pre-defined password length.

7.2.4d Resource Link

The schemes administration application passwords are configured by BSG and require a combination of alphanumeric characters and a pre-defined password length.

7.2.4e Altair

The schemes administration application passwords are configured by BSG and require a combination of alphanumeric characters and a pre-defined password length.

7.2.4f Profund Classic

The schemes administration application passwords are configured by the Pensions System Manager to contain any combination of alphanumeric characters, they cannot contain symbols and must be a minimum pre-defined password length.

7.2.4g Profund oPEN2

The schemes administration application passwords are defined at an AD level and configured by XPS IT or the Pensions System Manager and require a combination of alphanumeric characters and a pre-defined password length.

Auditor testing and results

Inspected the password parameters configured for each in-scope system. Noted that password requirements were configured in-line with the organisational requirements, requiring a combination of alphanumeric characters and a pre-defined password length.

No exceptions noted.

7.2.5a-7.2.5g Process

Application Lockouts

User accounts are locked out after a set number of failed attempts to authenticate requiring the user to contact the BSG via the XPS IT or BSG Helpdesk, telephone, email or in person to enable the account to be unlocked or reset.

Control

7.2.5a Compendia

Application accounts are locked out after three failed attempts at access. Accounts are unlocked by a member of the BSG Helpdesk on receipt of a request from the user.

7.2.5b Penscope

The schemes administration application accounts are defined at an AD level and are therefore locked out after three failed attempts at access. Accounts are unlocked by a member of the XPS IT Helpdesk on receipt of a request from the user.

7.2.5c Alfresco

The schemes administration application accounts are defined at an AD level and are therefore locked out after three failed attempts at access. Accounts are unlocked by a member of the XPS IT Helpdesk on receipt of a request from the user.

7.2.5d Resource Link

Application accounts are locked out after three failed attempts at access. Accounts are unlocked by a member of the XPS IT or BSG Helpdesk on receipt of a request from the user.

7.2.5e Altair

Application accounts are configured to be locked out after three failed attempts at access. Accounts are unlocked by a member of the BSG on receipt of a request from the user.

7.2.5f Profund Classic

Application accounts are locked out after three failed attempts at access. Accounts are unlocked by a member of the XPS IT Helpdesk on receipt of a request from the user.

7.2.5g Profund oPEN2

The schemes administration application accounts are defined at an AD level and are therefore locked out after three failed attempts at access. Accounts are unlocked by a member of the XPS IT Helpdesk on receipt of a request from the user.

Auditor testing and results

For each in-scope system, inspected the lockout parameters configured. Noted that, for applications which do not rely on the Active Directory, application accounts were configured to be locked out after three failed attempts.

For applications which rely upon the Active Directory, inspected the domain lockout parameters as part of control 7.2.2 (non-Altair).

Unlock requests have been tested as part of control 7.2.2 (non-Altair).

No exceptions noted.

7.2.6-7.2.7 Process

Provisioning of Users: Network User Accounts

Add and Change a user administration process to add and change user accounts, security groups or other system objects is instigated, assessed and authorised by business areas using new starter forms or employee change of details forms. The business will detail which systems resources the user can access and their access rights to each. The request is recorded in the IT Services help desk and may be further authorised as required by the XPS IT Management.

Control

7.2.6 Network User Accounts: Add

Requests to add user accounts are submitted and approved by a business representative to the IT Services Helpdesk.

Auditor testing and results

For a sample of new starters, inspected the service desk ticket submitted to the IT Services help desk. Noted that requests were submitted and approved by a business representative.

No exceptions noted.

Control

7.2.7 Network User Accounts: Change

Requests to change user accounts are submitted to the IT Services Helpdesk by a business representative and actioned upon authorisation from the XPS IT Management.

Auditor testing and results

A suitable system-generated or manually-maintained population for this control was unable to be obtained for sampling. As such, this control could not be tested, therefore, an exception is noted.

Exception noted.

Management response:

As we did not have a formally documented movers process in place during 2021, we were unable to provide RSM with a suitable system generated population of requests to change user accounts during the audit period.

Whilst we were able to provide a population of account changes to RSM through lists provided by our HR Team, we note that significant manual alterations and explanations were required to these lists, meaning that RSM were unable to gain confidence that an accurate list of user account changes had been provided.

We are currently implementing a new process through our HR Team and ServiceNow IT Helpdesk, which will enable us report more easily on requests to change user accounts. We expect this process to be implemented by the end of Quarter 2 2022.

7.2.8 Process

Network User Accounts: Disable and Remove

Notification of a terminated employee is submitted by an authorised business representative to the IT Services Helpdesk via a staff leaver request. User accounts are disabled or with business authorisation will remain active for an agreed period. A review of all accounts takes place annually with a monthly report set to go to the XPS IT Management at the end of each month of inactive accounts.

Control

Notifications of terminated employees are sent to the IT Services Helpdesk by a business representative upon completion of a leaver form. The user accounts are either disabled immediately, if the termination date has passed and no authorisation to remain has been agreed or, with business authorisation, remain active for an agreed period after which time the account is closed.

Auditor testing and results

For a sample of leavers, inspected the service desk ticket raised.

For three of the leavers tested, no corresponding ticket or form was able to be provided, therefore an exception was noted.

Exception noted.

For two of these, inspected the last logon date to the account, and noted that this was prior to the leave date, and therefore this access has not been exploited.

However, for the remaining account, noted that the last logon date was one day after the HR leave date. Enquired of management and inspected corroborating email evidence, and noted that permission had been given for this user to login on this date to complete outstanding tasks. Noted that this access has therefore not been exploited.

Noted from enquiry with management that changes to the internal processes for this control were made during the in-scope period. No exceptions were noted for sampled leavers with leave dates after these changes were made.

Management response:

We were unable to locate evidence of a request being sent to remove access to the XPS IT network with relation to 3 of the 25 employees reviewed. We have noted that access was removed in a timely manner upon these employees leaving XPS. In 2 of the 3 cases the last logon date was prior to the users' leave dates and therefore this access was not exploited. In 1 case the last logon date was 1 day after the leave date, however we are satisfied that appropriate permission had been granted to the user to login on this date to complete outstanding tasks.

In addition to our standard leaver process, we carry out checks on a weekly basis to ensure that access has been removed appropriately, with an emergency leaver form issued where access had not been removed. Access was removed through this process, for 6 of the 25 leavers sampled.

We have implemented a new system-integrated leaver form, with effect from October 2021. We have noted that the above exceptions relate to the period prior to this process. RSM have carried out additional testing following the implementation of our new process, and found no exceptions to this process post-October 2021.

We are also currently carrying out an internal audit of all company leavers during Quarter 1 2022, to ensure that access has been removed appropriately and that our new process is functioning effectively.

7. Restricting access to systems and data

7.3 Client and third party access to in-scope systems and data is restricted and/or monitored

7.3.1 Process

Access to XPS applications is granted in line with the 3rd party access request guide (for external vendors) the 3rd Party vendor management process and the 3rd party vendor Password Reset Procedure, for the following suppliers:

- › ITM
- › Zellis
- › Synapps
- › Littlefish
- › Bottomline

Control

Access to XPS applications is granted in line with the 3rd party access request guide (for external vendors) the 3rd Party vendor management process and the 3rd party vendor Password Reset Procedure, for the following suppliers:

- › ITM
- › Zellis
- › Synapps
- › Bottomline

Where the new supplier requires access to an XPS application, this must be requested by an approved member of XPS Management through completion of an External Vendor Access Request form which is submitted to the IT Helpdesk. This must confirm the access method and type of access required.

The request is reviewed and approved by the IT Operations Manager, IT Security Manager and Head of Risk. Access may either be restricted or denied by either XPS IT or XPS Risk. Any decision by the IT Operations manager or IT Security Manager may only be overturned by the IT Director, whilst any decision by the Head of Risk may not be overturned.

Where an existing vendor requires access to an XPS application, this must be requested via an authorised XPS employee. XPS IT will confirm that the employee requesting access for the vendor is authorised before granting access.

Access is time limited to Monday to Friday 8AM to 6PM and set to expire after 7 days.

If access is required outside of Monday to Friday 8AM to 6PM, then the XPS 3rd party contract owner will need to authorise the request.

Approved 3rd party vendors log in to the XPS application via Cisco AnyConnect. The user account is set to expire the user account after 60 days in line with the XPS password policy. Any password resets are activated in line with the 3rd party vendor Password Reset Procedure.

Auditor testing and results

Inspected third-party vendor policy and procedure documentation and noted that vendor management and vendor password reset and activation procedure documentation was in place. For a sample of vendor access requests, inspected the ticket raised and associated email evidence, and noted that they had been actioned in line with the documented procedure.

No exceptions noted.

7.3.2 Process

The supplier is able to access the XPS network directly via a client installed on their management servers.

Control

Access to data within the XPS domain is limited through network controls in place. Quarterly access reviews are carried out to ensure that access remains appropriate.

Auditor testing and results

Inspected the population of users from the supplier, and noted that these were restricted to unique accounts limited through the network controls. For a sample of quarters, inspected the access review minutes and noted that quarterly access review meetings had been held.

No exceptions noted.

7.3.3 Process

The supplier provides data centre services to XPS and has direct access to the XPS network via Cisco Any Connect.

Control

Access to the XPS data is restricted via access controls, the supplier has access to the XPS core network but do not have Active Directory Accounts or access to servers or files.

Auditor testing and results

Inspected the configuration of access to the network by the third-party, and noted that supplier users had access to the core network, but no access to Active Directory, servers or files. No exception noted.

No exceptions noted.

7. Restricting access to systems and data

7.4 Segregation of incompatible duties within and across business and technology functions is formally defined, implemented, updated and enforced by logical security controls

7.4.1 Process

The Outsourced IT Provider’s Administrators carry out multifunction roles, including the creation of AD accounts and password resets, and as such have access to all the relevant areas of the network (but not to business systems). This allows them to carry out their duties fully even when “on call”.

Control

On a monthly basis, meetings are held between the Outsourced IT Provider and XPS Administration to discuss the services provided by the Outsourced IT Provider including access to the XPS Administration network and are evidenced by meeting minutes.

Auditor testing and results

For a sample of months, inspected the minutes of service review meetings with outsourced IT providers. Noted that monthly service review meetings were held and evidenced by minutes.

No exceptions noted.

7.4.2 Process

Pensions Administration Users

Access to the scheme's administration application is controlled by username and password. Associated with each Pensions Administrator is a security profile which determines:

- › The relevant schemes to which they have access
- › The functionality they can access
- › The member records they can access
- › Whether they are permitted to amend data or view data only, access by an IT Applications Team Support

Analyst requires entry of a unique username and password into a separate security database. (Control 7.3.2) Built into the scheme's administration application are security procedures controlling access to sensitive data and facilities. The audit trail facility records changes made to the data, including who made the changes and when. (Control 7.3.3)

Control

7.4.2a Compendia Users

Segregation of duties rules are enforced by security profiles built into the scheme's administration applications. Profiles are assigned to authorised individuals, following an access request from a Team Leader or above, and are aligned to their job roles and responsibilities.

7.4.2b Penscope Users

Segregation of duties rules are enforced by security profiles built into the scheme's administration application. Profiles are assigned to authorised individuals by a Team Leader or above and are aligned to their job roles and responsibilities.

7.4.2c Alfresco Users

Segregation of duties rules are enforced by security profiles built into the scheme's administration applications. Profiles are assigned to authorised individuals, following an access request from a Team Leader or above, and are aligned to their job roles and responsibilities.

7.4.2d Resource Link Users

Segregation of duties rules are enforced by security profiles built into the scheme's administration applications. Profiles are assigned to authorised individuals, following an access request from a Team Leader or above, and are aligned to their job roles and responsibilities.

7.4.2e Profund Users

Segregation of duties rules are enforced by security profiles built into the scheme's administration applications. Profiles are assigned to authorised individuals by a Team Leader or above and are aligned to their job roles and responsibilities.

Auditor testing and results

For each in-scope system, inspected evidence of the configuration of segregation of duties and profiles. Noted that all applications enforced segregation of duties. Access requests for the in-scope applications have been tested as part of control 7.2.3.

No exceptions noted.

7.4.3 Process

Pensions Administration Users

Access to administration applications is controlled by username and password or by Single or Same Sign on with authentication via the Active Directory. Associated with each Pensions Administrator is a security profile which determines:

- › The relevant schemes to which they have access
- › The functionality they can access
- › The member records they can access
- › Whether they are permitted to amend data or view data only

Access by the IT Applications Team requires entry of a unique username and password into a separate security database. (Control 7.3.2) end data or view data only.

Built into the scheme's administration application are security procedures controlling access to sensitive data and facilities. The audit trail facility records changes made to the data, including who made the changes and when. (Control 7.3.3)

Control

7.4.3a Compendia Users

Access to the schemes administration application non-Production environments is restricted to the IT Applications Team and nominated Administration team users. Work is only undertaken on receipt of a Project log or Helpdesk request that has been authorised by a Team Leader or above. All actions are logged in the system and an audit trail is maintained.

7.4.3b Penscope Users

Access to the schemes administration application non-Production environments is restricted to the IT Applications Team and nominated Administration team users. Work is only undertaken on receipt of a Project log or Helpdesk request that has been authorised by a Team Leader or above. All actions are logged in the system and an audit trail is maintained.

7.4.3c Alfresco Support Users

Access to the schemes administration application non-Production environments is restricted to the IT Applications Team and nominated Administration team users. Work is only undertaken on receipt of a Project log or Helpdesk request that has been authorised by a Team Leader or above. All actions are logged in the system and an audit trail is maintained.

7.4.3d Resource Link Support Users

Access to the schemes administration application non-Production environments is restricted to the IT Applications Team and nominated Administration team users. Work is only undertaken on receipt of a Project log or Helpdesk request that has been authorised by a Team Leader or above. All actions are logged in the system and an audit trail is maintained.

Auditor testing and results

For each in-scope system, inspected the configuration of non-Production environments. Noted that these were logically separated from the Production environment and access restricted. Testing of changes and work undertaken in non-Production environments has been included in control 7.10.1.

No exceptions noted.

7.4.4 Process

Segregation of Application Environments

Live Production environments are located on separate servers. Production data changes are managed within the Business Services Group.

Control

a. Compendia/Altair/Profund

Production environments are logically separated from Test and Development environments.

b. Penscope, Alfresco and Resource Link

Production environments are logically separated from Test and Development environments.

Auditor testing and results

For each in-scope system, inspected the configuration of the Test and Development environments. Noted that these were logically separated from the Production environment.

No exceptions noted.

7. Maintaining integrity of the systems

7.5 Scheduling and internal processing of data is complete, accurate and within agreed timescales

7.5.1 Process (Compendia Clients only)

Batch processing, e.g. monthly allocations, payrolls etc. are scheduled and run by the Pensions Administration Team on an independent server, minimising the impact on Business as Usual.

Control

The Administration Team schedule the tasks in the diary of the scheme's administration application. These are then picked up by the ROBOT user/server. The Administration Team review the diary on a daily basis to verify that tasks have been run. Evidence that the task has been run is retained in the scheme's administration application diary.

Auditor testing and results

Inspected the configuration of the ROBOT service user and performed a walkthrough of the running of a task live. Noted that scheduled tasks are run by the ROBOT service user with an audit trail maintained to log completed tasks.

No exceptions noted.

7.5.2 Process

Batch processing, e.g. monthly allocations, payrolls etc. are scheduled and run by the Pensions Administration Team on an independent server, minimising the impact on Business as Usual.

Control

Any problems encountered with the ROBOT user/server are logged with the IT Applications Team via the Project Log or the Helpdesk system and allocated to an IT Applications Team member for resolution. Evidence of the problem and its resolution are retained within the Project log or the Helpdesk system.

Auditor testing and results

For a sample of ROBOT task failures, inspected the record logged with the IT Applications Team. Noted that task failures were logged and investigated to resolution, with evidence retained.

No exceptions noted.

7. Maintaining integrity of the systems

7.6 Transmission of data to/from external parties is complete, accurate, executed within agreed timescales and secure in line with external party agreements

7.6.1 Process

Transmissions of bulk data by XPS to clients are made via a secure website facility or via encrypted e-mail.

Control

Where the secure transfer site is used:

- › Only authorised users are able to upload and transfer data.
- › Users are provided with unique login credentials to access data.
- › User access within the transfer site is restricted to authorised folders.

Where data is sent by e-mail, this is encrypted either using Winzip or an encrypted spreadsheet or Word document.

Auditor testing and results

Inspected the configuration of the secure transfer site and noted that access is restricted to authorised users who require unique credentials to access authorised folders.

Inspected the configuration of the Data Loss Prevention solution and noted that the tool blocked the sending of unencrypted emails containing sensitive data.

No exceptions noted.

7.6.2 Process

Outbound e-mails are scanned using the Mimecast Data Loss Prevention tool, to prevent non-encrypted personal data from being sent.

Control

The Mimecast Data Loss Prevention tool is used to scan outbound email communication to prevent non-encrypted personal data from being sent.

Auditor testing and results

The Mimecast Data Loss Prevention tool is used to scan outbound email communication to prevent non-encrypted personal data from being sent.

No exceptions noted.

7.6.3 Process

TLS encryption is automatically enforced on inbound and outbound e-mails to protect the confidentiality and integrity of data in transit.

Control

TLS 1.2 encryption is automatically enforced on inbound and outbound emails.

Auditor testing and results

Inspected the configuration of the email solution and noted that TLS 1.2 encryption was enforced on inbound and outbound emails.

No exceptions noted.

7. Maintaining integrity of the systems

7.7 Network perimeter security devices are installed and changes are tested and approved

7.7.1 Process

A number of control measures are deployed by Backbone to protect the organisation from malicious attack. Firewalls which control inbound and outbound traffic are maintained by Backbone. Changes to the Firewalls will be made either in response to an incident or through an authorised change process signed off by the XPS IT Management. Backbone monitors the Firewalls and reports on threats to the XPS IT Management.

Control

In/outbound traffic is controlled through the implementation of Firewalls. Changes to the Firewall Rules are signed off by XPS IT Management or the Technical Lead prior to implementation.

Monthly Service Review meetings are held between XPS Administration and the Outsourced IT Provider to discuss services provided and minutes of the meetings are retained.

Auditor testing and results

For a sample of firewall changes, inspected change documentation and noted that changes were signed off by IT Management or the Technical Lead prior to implementation.

For a sample of monthly, inspected the meeting minutes and noted that service review meetings were held with the outsourced IT provider with minutes retained.

No exceptions noted.

7.7.2 Process

A Penetration Test of the security perimeter is conducted by a specialist supplier at least every 12 months. A report is produced which contains any perceived vulnerabilities. Any changes are raised through the change process to be assessed and remediated by the appropriate technical staff.

Control

A Penetration Test of the external network security is conducted at least every 12 months. Findings are raised in a Management report and any changes are discussed with XPS IT Management via email and then logged via the change management process for the appropriate actions to be taken.

Auditor testing and results

Inspected the annual penetration test report and noted that an annual penetration test had been carried out with findings recorded and actioned.

No exceptions noted.

7. Maintaining integrity of the systems

7.8 Anti-virus definitions are periodically updated across all terminals and servers, deployment and settings are periodically reviewed and updated when required; and patterns of attempted external breaches are monitored

7.8.1-7.8.3 Process

IT Projects

Anti-virus, Anti-Malware and Internal E-Mail Scanning Internally, Webroot secure anywhere is deployed to provide protection for servers, workstations and laptops against viruses, spyware and to provide proactive protection against unknown threats. Externally, a specialist supplier is used to scan for viruses, malicious content and SPAM. (Control 7.6.5) Internally, additional rule sets are configurable by IT Services to either allow or reject attachments for defined file extensions. Files definitions and scan engines are automatically updated as per vendor specifications. (Control 7.6.3) All laptops are encrypted. (Control 7.6.4)

Control

7.8.1 Webroot Secure Anywhere is configured to provide protection for servers, workstations and laptops against viruses, spyware and to provide proactive protection against other new threats.

Auditor testing and results

Inspected the configuration of the anti-virus and anti-malware solution. Noted that the application was configured for proactive protection and to automatically update threat definitions.

No exceptions noted.

Control

7.8.2 All laptops are encrypted. Laptop encryption cannot be disabled by non IT admin users.

Auditor testing and results

Inspected the configuration of the encryption solution and noted that encryption was enabled. Performed a walkthrough of a non IT admin user attempting to disable the encryption and noted that the user could not disable the encryption.

No exceptions noted.

Control

7.8.3 Externally, a specialist supplier is used to scan for viruses, malicious content and SPAM. Internally, additional rule sets are configured by IT Services to either allow or reject attachments for defined file extensions.

Changes to the rule set are informed to the IT Provider, by XPS IT Management, using the Change Management process. The software automatically alerts the Helpdesk if a threat is identified, and action is taken. Any such threats will be reported to XPS IT Management and raised at the monthly Service Review meetings. Threats identified are logged into threat history and retained for 90 days.

Auditor testing and results

Inspected the scanner configuration and noted that it was configured to scan for viruses, malicious content and SPAM, with additional parameters for attachments and file extensions, along with retention of threat logs and automatic alert configuration.

No exceptions noted.

7. Maintaining integrity of the systems

7.9 Data received from external parties is scanned for known vulnerabilities, any compromised data is quarantined, and definitions of threats are periodically updated

7.9.1-7.9.3 Process

See 7.6.1, 7.6.2, 7.6.3

Control

See 7.6.1, 7.6.2, 7.6.3

Auditor testing and results

Tested as part of controls 7.6.1, 7.6.2, and 7.6.3.

7. Maintaining and developing systems hardware and software

7.10 Development and implementation of both in house and third party in-scope systems are authorised, tested and approved

7.10.1a Process

Compendia: Production Data and Configuration Changes

When a limited number of data amendments changes are required to the schemes administration application the request is raised by the Administration Team through the IT Applications Team Helpdesk or added to the Project Log and approved by a Senior Administrator. Scheme specific checklists are added to the Helpdesk system as appropriate.

The IT Applications Team review and makes the individual changes directly, with an audit trail being retained within the database logs of the changes made.

The Pension Administrator reviews that the changes made are appropriate and the Helpdesk ticket is signed off and closed by either the Pension Administrator or an IT Applications Team System Analyst.

Control

For data amendment and configuration changes made to Compendia, the Administration Team raise a request with the IT Applications Team through the IT Applications helpdesk or the Project log.

The Pensions Administration Team conducts user acceptance testing (UAT) and retains evidence of test results.

Changes are approved by a senior administrator prior to the change release into the live environment.

Auditor testing and results

For a sample of changes, inspected the request raised. Noted that approval and UAT sign-off was received prior to implementation and test results retained.

No exceptions noted.

7.10.1b Process

Production Data Changes

Request for data amendments for existing schemes are raised by an Administrator with the IT Applications Team via the IT Applications Helpdesk system or added to the Project Log.

The changes are assessed by the IT Applications Team and actioned by an the IT Applications Administrator or referred to the 3rd party application provider to progress the change. Changes referred to 3rd parties are logged on the 3rd party ticketing system.

Control

For Penscope, Alfresco or Resource Link, data amendments are applied to non-production environments by the IT Applications Team or the third party application providers. These are tested by an IT Applications Team Administrator and signed-off by an Administration Manager or Administrator prior to release to the Live environment.

Updates to the originator are provided via the Helpdesk System or Project Owner.

Auditor testing and results

For a sample of changes, inspected the log and noted that data amendments were applied to non-production environments by the IT Application Team or the third party application providers, and sign-off was received prior to implementation into the Live environment.

Inspected the configuration of the Helpdesk System and noted it was configured to automatically send updates to the originator.

No exceptions noted.

7.10.1c Process (Profund only)

For the Profund system used by the Bristol Cote House office, no development is carried out. Mandatory updates are applied to the software where required by the third party application provider, for example due to changes to regulatory requirements.

Control

The Pensions Systems Manager applies the mandatory updates to the software where required by the third party application provider. The Pensions System Manager takes a back-up of the system before the update is applied, to help ensure that data can be recovered in case of any issues when applying the patch.

Auditor testing and results

Inspected the application configuration and noted that mandatory updates from the provider were applied.

Inspected the configuration of backups for the application and noted that backups were taken on a daily basis to ensure that a back-up has always been performed prior to the implementation of a mandatory update, with a retention policy applied.

No exceptions noted.

7.10.2 Process

Authorisation of Development of New Client Pensions Administration Systems

New clients are added to the existing application environment. See controls in section 1 – Accepting Clients.

Control

See controls in Section 1 – Accepting Clients.

Auditor testing and results

See controls in Section 1 – Accepting Clients.

7. Maintaining and developing systems hardware and software

7.11 Data migration or modification is authorised, tested and, once performed, reconciled back to the source-data

7.11.1 Process

For the majority of clients our Pensions Administration technologies have not required migration or modification of data in recent years. Any such modifications would follow our Change Management procedures as described in the section Maintaining and Developing Systems Hardware and Software. Any migrations that have taken place have followed a comparable process and control set as for new Scheme Implementations (Section 1 - Accepting Clients). A Project Team is set up to manage the migration. The team is sponsored by a representative from Senior Management and is managed by a dedicated Project Manager. A Project Board is established to govern the project. The Project Team consists of a number of individual work streams. The Project is managed as a PRINCE 2 project, in accordance with XPS Administration standards and procedures. The project is managed according to a formal Project Plan. The Project Plan is populated with key project milestones and target dates that have been agreed with the Client, evidence of this agreement is retained by the Project Manager.

Control

At least monthly, the Project Board monitors the progress of the approved Project Plan. Any issues relating to progress are discussed with the Project Manager and the Client. Meeting minutes are taken, which include any agreed actions, distributed to all meeting participants and retained in the Project Library by the Project Manager. Acceptance of Client set up details and any additional actions required after the go live date are approved by the Service Delivery Manager and Project Manager signing off the Migration Report by e-mail. The completed Migration Report and any supporting e-mails are retained by the Project Manager in the Project Library.

Auditor testing and results

For a sample of migrations, inspected the associated documentation and noted that the project had been appropriately signed off and closed, with documentation retained.

No exceptions noted.

7.11.2 Process

The Project Manager tracks the milestones to verify that they are completed on time and to a standard agreed with the Client and provides regular progress reports to the Project Board and Client. The Project Plan varies according to the specific requirements of each transaction. The Project Manager prepares a Go Live Migration Report which includes Migration Summary results, Client data records, details of any outstanding issues remaining at go live along with member and any unit reconciliations. By signing off the Migration Report in hardcopy or via email the Pensions Administration Team confirm that they have a complete understanding of the scheme and can deliver services according to the Client Agreement and Regulatory and legislative Requirements.

Control

Prior to commencement of Administration services on a new System, the Systems Pensions Analyst reconciles Scheme data provided from the previous system to the new system and raises any exceptions regarding missing or incorrect data with the Pensions Administration Team. Reports generated by the data audit, along with any correspondence to resolve any data gaps or errors are held centrally in the Project library.

Auditor testing and results

For a sample of migrations, inspected evidence of reconciliations performed and noted that data reconciliation had been carried out with any exceptions investigated to conclusion.

No exceptions noted.

7.11.3 Process

As part of the project, Scheme data is audited, with any queries being raised with the Pensions Administration Team. The data is analysed using a data migration tool, which generates reports that identify any gaps or errors in the data received.

Control

Scheme data reconciliations and correspondence relating to the follow up of any gaps or errors identified are verified by a member of the Project Team and evidenced by sign off on the Implementation Control Sheet. Copies of the Implementation Control Sheet are retained in the Project Library.

Auditor testing and results

For a sample of migrations, inspected evidence that data had been reconciled and that errors identified had been investigated and followed-up to completion. Progress of the migration, including notes on errors, were recorded in the Implementation Control Sheet.

No exceptions noted.

7. Maintaining and developing systems hardware and software

7.12 Changes to existing in-scope systems, including hardware upgrades, software patches and direct configuration changes, are authorised, tested and approved in line with policy

7.12.1 Process

IT Projects

The initiation of an IT project requires authorisation from XPS IT Management. Where capital investment is required, it will also have a business case, otherwise a statement of requirements. Each project has a sponsor. Project implementation requires approval from the XPS IT Management.

Control

Project initiation requires Business Authorisations by e-mail from the XPS IT Management. The project is measured via monthly Service Review meeting minutes. Internal projects are monitored throughout via monthly meetings to discuss progress against milestones. Project updates are produced and retained in the project file which is accessible by Management.

Auditor testing and results

This control could not be tested as there were no applicable projects during the period.

7.12.2a Process

Application Configuration Changes

Requests for configuration changes to existing systems are raised by an Administrator with the IT Applications Team through the IT Applications Helpdesk system or added to the Project Log.

The changes are assessed by the IT Applications Team and actioned by an IT Applications Team resource or referred to the 3rd party application provider to progress the change. Changes referred to 3rd parties are logged on the 3rd party ticketing system.

Control

For Penscope, Alfresco or Resourcelink, application configuration changes are applied to non-production environments by the IT Applications Team or the Third Party application providers. These are tested by an IT Applications Administrator and signed-off by an Administration Manager or Administrator prior to release to the Live environment.

Updates to the originator will be provided via the Helpdesk System or Project Owner, who will also obtain the relevant authorisations for sign-off before release to Live.

Auditor testing and results

For a sample of changes, inspected the change documentation and noted that configuration changes were applied to non-Production environments by the IT Applications Team or the Third Party application providers, tested by an IT Applications Administrator and signed-off by an Administration Manager or Administrator prior to release to the Live environment, with updates and sign-offs provided to the originator.

No exception noted.

7.12.2b Process (Altair)

Application Configuration Changes

Requests for configuration changes to existing systems are raised by an Administrator with the 3rd party application provider.

The changes are assessed by the 3rd party application provider to progress the change. Changes referred to 3rd parties are logged on the 3rd party ticketing system.

Control

Application configuration changes are applied to a Test environment by the Third Party application providers. These are tested and signed off by the Systems Manager prior to release to the Live environment.

The Systems Manager signs off completion of the change once it has been released to a Live environment.

Auditor testing and results

For a sample of changes, inspected the change documentation and noted that configuration changes were applied to a test environment by the third party application providers, tested and signed off by the Systems Manager prior to release, and signed off for completion following implementation.

No exception noted.

7.12.3a Process

Software Changes

Functional or Application changes or scheme calculation releases generate a “Software Release”. New or amended application code is released to the Live environment by the IT Applications Team to support the following business requirements:

- › Releases of new of amended client specific benefit calculations
- › The first time loading of client databases into the Live environment.
- › Workflow functionality.

Control

Approval for Compendia software changes by the IT Applications Team to the Live Production Systems are formalised through a signoff by the Administration Product Owner or Administration Team Manager and either recorded in the Work Management System or received via e-mail.

Auditor testing and results

This control could not be tested as there were no applicable changes during the period.

7.12.3b Process (Altair)

Software Changes

Functional or Application changes or scheme calculation releases are released to the Live environment by the Third Party application provider to support the following business requirements:

- › Releases of new of amended client specific benefit calculations
- › The first time loading of client databases into the Live environment.
- › Workflow functionality.

Control

Approval for Altair software changes by the third party application provider to the Live system are formalised through a signoff by the Systems Manager. These are recorded in the third party application provider’s Work Management System.

Auditor testing and results

For a sample of changes, inspected the change documentation and noted that software changes were signed off by the Systems Manager prior to release, and signed off for completion following implementation.

No exception noted.

7.12.3c Process

Software Changes

Functional Application changes including application upgrades and scheme calculation changes are managed by the IT Applications Team as a release package supported by application suppliers and the XPS IT Team. Release packages may contain the following:

- › XPS driven components:
 - › Releases of new or amended client specific benefit calculations – IT Applications Team
 - › The first time loading of client databases into the Live environment
 - › Client or XPS development requirements
- › 3rd Party/Legislative driven components:
 - › Supplier Roadmap items
 - › Mandatory Application upgrades

Control

For Penscope, Alfresco or Resourcelink, application software changes are developed as agreed between the IT Applications Team and the Third Party application providers and XPS IT where relevant. These are tested by an IT Applications Team Administrator and signed-off by a Pensions Administration Manager or Pensions Administrator prior to release to the Live environment.

Updates to the XPS Administration teams impacted by the change are provided prior to the change work commencing and once the change has been released to Live.

Auditor testing and results

For a sample of changes, inspected the change documentation and noted that the change was agreed with the third party application provider, tested by an IT Applications Team Administrator, signed-off by a Pensions Administration Manager or Pensions Administrator prior to release to the Live environment, and updates were provided to impacted teams.

No exception noted.

7.12.4 Process

Documentation

Documentation relating to testing is retained by either the Pensions Administration Team or the IT Applications Team. Documentation relating to authorisation and release is retained by the IT Applications Team.

Control

Software Releases are created by an approved third party software provider and signed off by the IT Applications Team. Documentation relating to the authorisation and release of changes is retained by the IT Applications Team.

Auditor testing and results

For a sample of changes, inspected the change documentation and noted that the change was agreed with the third party application provider, signed off by the IT Applications Team and documentation retained.

No exception noted.

7.12.5 Process

Core systems have documented operating procedures.

Control

Software Releases are created by an approved third party software provider and signed off by the IT Applications Team. Documentation relating to the authorisation and release of changes is retained by the IT Applications Team.

Auditor testing and results

For a sample of changes, inspected the change documentation and noted that the change was agreed with the third party application provider, signed off by the IT Applications Team and documentation retained.

No exception noted.

7.12.6 Process

IT Changes

IT services Change Management process follows the Information Technology Infrastructure Library (ITIL) framework. All proposed changes to the IT infrastructure Systems and Application Code releases will be classified as either:

- › Service Request (SR), which is submitted to IT Services
- › A Change Request (RFC) which is submitted to the XPS IT Management and captured and recorded via the Change Request with IT Services (Control 7.8.8)
- › Note: Service Requests are small repeatable operational changes. These include:
 - › New Starters and Leavers
 - › New/Change system access
 - › Backup/Restore requests
 - › Remote connectivity
 - › Approved software installs
 - › Approved DLL code releases

Control

IT changes – Service Requests (SR's):
Service Requests (SR's) are submitted to IT Services. Each SR is assigned a unique identification number and held within the IT management system.

IT changes – Change Requests (RFC's):
Change Requests are submitted to IT Services Desk and referred on to the IT Management.

Auditor testing and results

For a sample of service requests and change requests, inspected the request ticket. Noted that each request was assigned a unique identification number, held within the ticketing system and referred to IT Management.

No exception noted.

7.12.7 Process

Change Implementation, Resolution and Closure

Following implementation, change requests are set to “resolved” status by the Change Implementer within the IT Management Service Desk and the initiator will be informed. Emergency IT Changes are managed via IT Services Change Management Process and reported back to the XPS IT Management.

Control

Following implementation, change requests are set to “resolved” status by the Change Implementer within the IT Management Service Desk and the initiator informed. Emergency changes are managed via the IT Services Change Management Process and reported back To the XPS IT Management on completion.

Auditor testing and results

For a sample of changes, inspected the ticket and noted that requests were set to “resolved” status following implementation with the initiator informed. Noted that emergency changes followed the IT Services Change Management Process and were reported back to the XPS IT Management upon completion.

No exception noted.

7. Recovering from processing interruptions

7.13 IT related Disaster Recovery Plans are documented, updated, approved and tested

7.13.1 Process

XPS Administration's Business Continuity Plans are prepared and maintained by the respective Plan Coordinators and approved and signed off by the respective Plan Owners. The Framework and Policy are aligned with ISO22301. The principal accountabilities of ongoing business continuity management are as follows:

- › Review the current business continuity policy documentation to ensure it reflects a Group wide approach
- › Review scenario planning for the business and IT operations and incorporates a minimum set of likely occurrences into the reviewed business continuity policy
- › Support the completion of all plans from all business areas aligned to the revised policy.

Control

Business Continuity Plans are prepared for each business line. These plans are formally reviewed, by the Risk team and the local offices on a yearly basis and updated as appropriate. Changes to the document are shown by a version number and date on the document.

The plans are tested on an annual basis. After the test, Business continuity plan owners produce a testing scenario report to confirm testing against the plan and highlighting any improvement actions.

Auditor testing and results

Inspected the Business Continuity Plans and noted that these were reviewed and updated on an annual basis, with version control documented.

Inspected evidence of the most recent Business Continuity Plan test, and noted that the annual test of the plans had been completed with a testing scenario report completed.

No exceptions noted.

7.13.2 Process

XPS Administration maintains a Business Systems Priorities register which confirms Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). These are tested at least annually to verify that relevant information can be recovered.

Control

IT related Disaster Recovery Plans are documented in the Business Systems Priority register. These are tested at least annually to verify that relevant information can be recovered.

Auditor testing and results

Inspected evidence of the most recent Disaster Recovery test and noted that the annual test of the plans had been completed.

No exceptions noted.

7. Recovering from processing interruptions

7.14 In-scope systems and data are backed up and tested such that they can be restored completely and within agreed timescales

7.14.1 Process

Infrastructure layer controls operated at the IT Services

Systems, databases and data are backed up according to a predefined schedule via automated tools. The backup cycle incorporates daily, monthly and annual backups. An issues log is maintained in respect of backups which fail or are incomplete. Failed or incomplete backups are investigated and reported to XPS IT Management on a daily basis. Recoverability of data files is tested at least annually by the Outsourced IT provider along with adhoc restores which are logged via IT service desk.

Control

Systems, databases and data are backed up according to a predefined schedule via automated tools. The backup cycle incorporates daily, weekly, monthly and yearly backups. Daily backups are retained for one week, monthly for one year and yearly for seven years. Backup failures are recorded for 30 days and are automatically sent to DPM console which is checked as part of IT daily checks.

Auditor testing and results

Inspected the backup configuration and noted that a backup cycle was configured, including retention period, and failures recorded and checked.

No exception noted.

7.14.2 Process

Application layer controls operated at the IT Services

Production Database Backups: Local online backups of databases and transactions logs. Local online backups of databases and transaction logs are taken on an hourly basis throughout the day in order to provide a more granular and speedy recovery time objective.

Control

Local online backups of databases and transaction logs are taken on an hourly basis throughout the day in order to provide a more granular and speedy recovery time.

Auditor testing and results

Inspected the backup configuration and noted that backups for databases and transaction logs were configured to run on an hourly basis.

No exceptions noted.

7.14.3 Process

Infrastructure and Application layer controls operated by IT Services

Recovery of data files is undertaken by XPS IT Services via ad hoc file recoveries in response to notifications received by their service desk.

Control

Recoverability of data files is undertaken by IT Services in response to notifications received by the Service Desk, who:

- › restore files to users;
- › confirm closure of corresponding incident records within the Service Management System.

Auditor testing and results

For a sample of file restoration requests, inspected the ticket logged and noted that the Service Desk restored the file(s) and confirmed closure of the corresponding incident records.

No exception noted.

7.14.4 Process

Infrastructure and Application layer controls operated by IT Services: IT Services calculates the remaining free space within each database instance and provides the information to the XPS IT Management for review and action where necessary.

Control

The remaining disk space within each database instance is monitored proactively using the network monitor tool. Automated tickets are generated by the tool within the IT outsourced service provider's helpdesk system when the remaining disk space falls below the expected thresholds. The outsourced IT service provider will investigate the issue and close the ticket as an evidence of addressing the issue.

Auditor testing and results

Inspected the configuration of the network monitoring tool and noted that it was configured to proactively alert when specific percentages of disk space remained. For a sample of automated tickets generated, inspected the ticket and corresponding documentation trail and noted that the outsourced service provider investigated the issue and closed the ticket.

No exception noted.

7. Recovering from processing interruptions

7.15 Problems and incidents relating to in-scope systems are identified and resolved within agreed timescales

7.15.1 Process

The IT service desk is a single point of contact for:

- › User incidents
- › User accounts, security groups and other system objects
- › Service requests
- › Software installations and modifications
- › Hardware incidents
- › Any IT security issues or threats Incidents and requests are subject to lifecycle management.

They are:

- › Investigated and diagnosed
- › Progressed, updated and actively monitored in line with their resolution target
- › Either resolved by the implementer/fixer at source or assigned to the relevant IT Services representative
- › Where necessary, are escalated internally and supplemented by management intervention where appropriate and as required by the requester Once resolved IT Services will contact the requester to seek authorisation for closure. Resolution targets are monitored by IT Services and reported to XPS IT Management on a monthly basis.

Control

Users are able to log calls to the IT Service Desk either by phone or email. Incidents are either resolved by the first line point of contact or logged into a queue for a member of second line support to pick up. Each incident is assigned a unique ID and a priority.

Auditor testing and results

For a sample of incidents, inspected the ticket logged and noted that the incident was assigned a unique ID and priority, and either resolved by first line or logged in a queue for second line support.

No exception noted.

7. Managing and monitoring compliance and outsourcing

7.16 Outsourced activities provided by Subservice Organisations are governed by contracts and service level agreements that are authorised and subject to regular review

7.16.1 Process

Management and Monitoring

A contract is in place for key outsourced service providers that includes an agreed schedule of services and defined service levels.

Control

Contracts and service level agreements are agreed at service take-on and reviewed either at the end of the term or when changes to the service occur. Changes are agreed between XPS and the subservice organisation.

Auditor testing and results

For a sample of service providers, inspected the contracts and noted that signed contracts were in place with agreed service levels. Management confirmed that, for the selection of contracts, no changes had been required during the period.

No exception noted.

7. Managing and monitoring compliance and outsourcing

7.17 The services provided by Subservice Organisations are regularly monitored and assessed against the standards set out in the service level agreements

7.17a-7.17h Process

Governance meetings are scheduled monthly to review the outsourced services for key suppliers against the agreed service levels.

Control

7.17a ITM

Governance meetings are scheduled monthly to review the outsourced services against the agreed service levels. Meetings include discussion of actions against agreed delivery dates and are minuted with the minutes distributed to the related parties. Performance is also monitored via live reporting available on the Confluence site.

Auditor testing and results

For a sample of monthly service meetings, inspected the minutes and noted that meetings were held, with reviewed actions agreed, and records were minuted.

No exception noted.

7.17b Zellis

Performance reports are provided on a monthly basis highlighting performance against agreed service levels and reviewed at monthly Governance meetings. Governance meetings include actions and agreed delivery dates and are minuted with the minutes distributed to the related parties.

For a sample of months, inspected the tracker for the service review meeting and noted that service review meetings were held, with performance reports provided and actions tracked.

No exception noted.

7.17c Synapps

Performance reports are provided on a monthly basis highlighting performance against agreed service levels and reviewed at monthly Governance meetings.

For a sample of months, inspected the monthly customer service report and noted that it had been provided by the third party and reviewed in the service meeting.

No exception noted.

7.17d CashFac

Performance statistics are provided on a monthly basis highlighting performance against agreed service levels and reviewed at monthly Governance meetings along with ongoing projects.

For a sample of months, inspected the monthly customer service report and noted that it had been provided by the third party and reviewed in the service meeting.

No exception noted.

Control

7.17e Bottomline

Performance reports are provided on a monthly basis highlighting performance against agreed service levels and reviewed at monthly Governance meetings.

Auditor testing and results

For a sample of months, inspected the monthly customer service report and noted that it had been provided by the third party and reviewed in the service meeting.

No exception noted.

7.17f Littlefish

Performance statistics are provided on a monthly basis and reviewed at monthly Governance meetings. Governance meetings include actions and agreed delivery dates and are minuted with the minutes distributed to the related parties.

For a sample of service meetings, inspected the minutes and noted that meetings were held with performance statistics reviewed, actions agreed, and records minuted.

No exception noted.

7.17g Backbone

Performance statistics are provided on a quarterly basis and reviewed at quarterly Governance meetings. Governance meetings include actions and agreed delivery dates and are minuted with the minutes distributed to the related parties.

For a sample of service meetings, inspected the minutes and noted that meetings were held with performance statistics reviewed, actions agreed, and records minuted.

No exception noted.

7.17h Adare

Governance meetings include a discussion of any ongoing performance issues and are minuted with the minutes distributed to the related parties.

For a sample of quarters, inspected the minutes of the quarterly meeting and noted that actions were minuted and tracked.

No exception noted.

Current issue date:
Expiry date:
Certificate identity number:

17 February 2022
10 January 2024
10428218

Original approval(s):
ISO/IEC 27001 - 11 January 2018

Certificate of Approval

This is to certify that the Management System of:

XPS Pensions Group PLC

Phoenix House, 1 Station Hill, Reading, RG1 1NB, United Kingdom

has been approved by LRQA to the following standards:

ISO/IEC 27001:2013

Approval number(s): ISO/IEC 27001 – 00011963

This certificate is valid only in association with the certificate schedule bearing the same number on which the locations applicable to this approval are listed.

The scope of this approval is applicable to:

Management of Information Security relating to the provision of pension administration and payroll services and the management of key third parties in accordance with the ISMS statement of applicability Version 2.n.

David Derrick

Area Operations Manager UK & Ireland

Issued by: LRQA Limited

LRQA Group Limited, its affiliates and subsidiaries and their respective officers, employees or agents are, individually and collectively, referred to in this clause as 'LRQA'. LRQA assumes no responsibility and shall not be liable to any person for any loss, damage or expense caused by reliance on the information or advice in this document or howsoever provided, unless that person has signed a contract with the relevant LRQA entity for the provision of this information or advice and in that case any responsibility or liability is exclusively on the terms and conditions set out in that contract.

Issued by: LRQA Limited, 1 Trinity Park, Bickenhill Lane, Birmingham B37 7ES, United Kingdom

Page 1 of 4



Certificate identity number: 10428218

Certificate Schedule

Location	Activities
Phoenix House, 1 Station Hill, Reading, RG1 1NB, United Kingdom	ISO/IEC 27001:2013 Management of Information Security relating to the provision of pension administration and payroll services and the management of key third parties in accordance with the ISMS statement of applicability Version 2.n.
1 Colmore Row, Birmingham, B3 2BJ, United Kingdom	ISO/IEC 27001:2013 Management of Information Security relating to the provision of pension administration and payroll services and the management of key third parties in accordance with the ISMS statement of applicability Version 2.n.
3rd Floor, Priory Place, New London Road, Chelmsford, CM2 0PP, United Kingdom	ISO/IEC 27001:2013 Management of Information Security relating to the provision of pension administration and payroll services and the management of key third parties in accordance with the ISMS statement of applicability Version 2.n.
3rd Floor, West Wing, 40 Torphichen Street, Edinburgh, EH3 8JB, United Kingdom	ISO/IEC 27001:2013 Management of Information Security relating to the provision of pension administration and payroll services and the management of key third parties in accordance with the ISMS statement of applicability Version 2.n.
Albion, Fishponds Road, Wokingham, RG41 2QE, United Kingdom	ISO/IEC 27001:2013 Management of Information Security relating to the provision of pension administration and payroll services and the management of key third parties in accordance with the ISMS statement of applicability Version 2.n.
Queens Quay, 33 - 35 Queens Square, Bristol, BS1 4LU, United Kingdom	ISO/IEC 27001:2013 Management of Information Security relating to the provision of pension administration and payroll services and the management of key third parties in accordance with the ISMS statement of applicability Version 2.n.



LRQA Group Limited, its affiliates and subsidiaries and their respective officers, employees or agents are, individually and collectively, referred to in this clause as 'LRQA'. LRQA assumes no responsibility and shall not be liable to any person for any loss, damage or expense caused by reliance on the information or advice in this document or howsoever provided, unless that person has signed a contract with the relevant LRQA entity for the provision of this information or advice and in that case any responsibility or liability is exclusively on the terms and conditions set out in that contract.

Issued by: LRQA Limited, 1 Trinity Park, Bickenhill Lane, Birmingham B37 7ES, United Kingdom



Certificate identity number: 10428218

Certificate Schedule

Location	Activities
Saltire House, 3 Whitefriars Crescent, Perth, PH2 0PA, United Kingdom	ISO/IEC 27001:2013 Management of Information Security relating to the provision of pension administration and payroll services and the management of key third parties in accordance with the ISMS statement of applicability Version 2.n.
4th Floor, Wellbar Central, Gallowgate, Newcastle, NE1 4TD, United Kingdom	ISO/IEC 27001:2013 Management of Information Security relating to the provision of pension administration and payroll services and the management of key third parties in accordance with the ISMS statement of applicability Version 2.n.
11 Strand, London, WC2N 5HR, United Kingdom	ISO/IEC 27001:2013 Management of Information Security relating to the provision of pension administration and payroll services and the management of key third parties in accordance with the ISMS statement of applicability Version 2.n.
Floor 2, 2 Centre Square, Middlesbrough, TS1 2BF, United Kingdom	ISO/IEC 27001:2013 Management of Information Security relating to the provision of pension administration and payroll services and the management of key third parties in accordance with the ISMS statement of applicability Version 2.n.
Office 48, Port View, One Port Way, Port Solent, Portsmouth, PO6 4TY, United Kingdom	ISO/IEC 27001:2013 Management of Information Security relating to the provision of pension administration and payroll services and the management of key third parties in accordance with the ISMS statement of applicability Version 2.n.
Cote House, The Promenade, Clifton, Bristol, BS8 3NG, United Kingdom	ISO/IEC 27001:2013 Management of Information Security relating to the provision of pension administration and payroll services and the management of key third parties in accordance with the ISMS statement of applicability Version 2.n.



LRQA Group Limited, its affiliates and subsidiaries and their respective officers, employees or agents are, individually and collectively, referred to in this clause as 'LRQA'. LRQA assumes no responsibility and shall not be liable to any person for any loss, damage or expense caused by reliance on the information or advice in this document or howsoever provided, unless that person has signed a contract with the relevant LRQA entity for the provision of this information or advice and in that case any responsibility or liability is exclusively on the terms and conditions set out in that contract.
Issued by: LRQA Limited, 1 Trinity Park, Bickenhill Lane, Birmingham B37 7ES, United Kingdom



Certificate identity number: 10428218

Certificate Schedule

Location	Activities
1 City Square, Leeds, LS1 2ES, United Kingdom	ISO/IEC 27001:2013 Management of Information Security relating to the provision of pension administration and payroll services and the management of key third parties in accordance with the ISMS statement of applicability Version 2.n.
1st Floor, Flax House, 83 - 91 Adelaide Street, Belfast, BT2 8FE, United Kingdom	ISO/IEC 27001:2013 Management of Information Security relating to the provision of pension administration and payroll services and the management of key third parties in accordance with the ISMS statement of applicability Version 2.n.



LRQA Group Limited, its affiliates and subsidiaries and their respective officers, employees or agents are, individually and collectively, referred to in this clause as 'LRQA'. LRQA assumes no responsibility and shall not be liable to any person for any loss, damage or expense caused by reliance on the information or advice in this document or howsoever provided, unless that person has signed a contract with the relevant LRQA entity for the provision of this information or advice and in that case any responsibility or liability is exclusively on the terms and conditions set out in that contract.
Issued by: LRQA Limited, 1 Trinity Park, Bickenhill Lane, Birmingham B37 7ES, United Kingdom



Current issue date: 7 February 2022
Expiry date: 6 February 2025
Certificate identity number: 10426152

Original approval(s):
ISO 14001 - 7 February 2022

Certificate of Approval

This is to certify that the Management System of:

XPS Pensions Consulting Limited

Phoenix House, 1 Station Hill, Reading, RG1 1NB, United Kingdom

has been approved by LRQA to the following standards:

ISO 14001:2015

Approval number(s): ISO 14001 – 00034669

This certificate is valid only in association with the certificate schedule bearing the same number on which the locations applicable to this approval are listed.

The scope of this approval is applicable to:

Management of office based environmental impacts supporting pensions administration, payroll services and other business services.

David Derrick

Area Operations Manager UK & Ireland

Issued by: LRQA Limited



LRQA Group Limited, its affiliates and subsidiaries and their respective officers, employees or agents are, individually and collectively, referred to in this clause as 'LRQA'. LRQA assumes no responsibility and shall not be liable to any person for any loss, damage or expense caused by reliance on the information or advice in this document or howsoever provided, unless that person has signed a contract with the relevant LRQA entity for the provision of this information or advice and in that case any responsibility or liability is exclusively on the terms and conditions set out in that contract.

Issued by: LRQA Limited, 1 Trinity Park, Bickenhill Lane, Birmingham B37 7ES, United Kingdom



Certificate identity number: 10426152

Certificate Schedule

Location	Activities
Phoenix House, 1 Station Hill, Reading, RG1 1NB, United Kingdom	ISO 14001:2015 Management of office based environmental impacts supporting pensions administration, payroll services and other business services.
4th Floor Wellbar Central , Gallowgate, Newcastle,, NE1 4TD, United Kingdom	ISO 14001:2015 Management of office based environmental impacts supporting pensions administration, payroll services and other business services.
Albion Fishponds Road, Wokingham,, RG41 2QE, United Kingdom	ISO 14001:2015 Management of office based environmental impacts supporting pensions administration, payroll services and other business services.



LRQA Group Limited, its affiliates and subsidiaries and their respective officers, employees or agents are, individually and collectively, referred to in this clause as 'LRQA'. LRQA assumes no responsibility and shall not be liable to any person for any loss, damage or expense caused by reliance on the information or advice in this document or howsoever provided, unless that person has signed a contract with the relevant LRQA entity for the provision of this information or advice and in that case any responsibility or liability is exclusively on the terms and conditions set out in that contract.
Issued by: LRQA Limited, 1 Trinity Park, Bickenhill Lane, Birmingham B37 7ES, United Kingdom

Appendix 2: Certificate of Assurance

**CYBER
ESSENTIALS
PLUS**

CERTIFICATE OF ASSURANCE
XPS Pensions Group Plc

COMPLIES WITH THE REQUIREMENTS OF THE CYBER ESSENTIALS PLUS SCHEME

NAME OF ASSESSOR : Yousef Abdulrahman

CERTIFICATE NUMBER : IASME-CEP-004419

PROFILE VERSION : April 2020

SCOPE : Whole organisation

DATE OF CERTIFICATION : 2021-06-30

RECERTIFICATION DUE : 2022-6-30

CERTIFICATION MARK


CERTIFICATION BODY


CYBER ESSENTIALS PARTNER


The Certificate certifies that the organisation was assessed as meeting the Cyber Essentials Plus implementation profile and thus that, at the time of testing, the organisation's ICT defences were assessed as satisfactory against commodity based cyber attack. However, this Certificate does not in any way guarantee that the organisation's defences will remain satisfactory against a cyber attack.

Appendix 3: XPS Engagement Letter



Our ref: JT/01-20/2021

Strictly Private & Confidential

The Directors
XPS Administration Limited
11 Strand
London
WC2N 5HR

25 Farringdon Street
London
EC4A 4AB
United Kingdom
T +44 (0)20 3201 8000
rsmuk.com

20 May 2021

To the Directors of XPS Administration Limited

INTRODUCTION

The purpose of this letter is to set out the basis on which we are to provide an assurance report in accordance with the Technical Release AAF 01/20 issued by the Institute of Chartered Accountants in England and Wales ('Service' or 'Services') and our respective areas of responsibility. Our services are provided in accordance with the attached Terms and Conditions of Business dated May 2018.

RESPONSIBILITIES OF SENIOR MANAGEMENT

Those charged with governance ('Senior Management') of XPS Administration Limited in relation to which the Service Auditors report is to be provided, are and shall be responsible for the design, implementation and operation of control activities that provide adequate level of control over pension administration services. Senior Management's responsibilities are and shall include:

- acceptance of responsibility for internal controls;
- evaluation of the effectiveness of the Service Organisation's control activities using suitable control objectives;
- supporting their evaluation with sufficient evidence, including documentation; and
- providing a written report ('Management Statement') of the effectiveness of the service organisation's internal controls for the relevant financial period.

In drafting this report Senior Management have regard to, as a minimum, the control objectives specified within the Technical Release AAF 01/20 issued by the Institute of Chartered Accountants in England and Wales ('ICAEW') but they may add to these to the extent that this is considered appropriate in order to meet User Entities expectations.

RESPONSIBILITIES OF REPORTING ACCOUNTANTS

It is our responsibility to form an independent conclusion, based on the work carried out in relation to the control activities of the Service Organisation's [describe Service Organisation's activity, pension administration services carried out at the specified business units of the Service Organisation located at Belfast, Birmingham, Bristol, Cheltenham, Edinburgh, Leeds, London, Middlesbrough, Newcastle, Perth, Reading, Wokingham as described in the Management's Statement and report this to Senior Management. An illustration of the form of our report is attached as Appendix 1.

THE POWER OF BEING UNDERSTOOD AUDIT | TAX | CONSULTING

RSM Corporate Finance LLP, RSM Legal LLP, RSM Restructuring Advisory LLP, RSM Risk Assurance Services LLP, RSM Tax and Advisory Services LLP, RSM UK Audit LLP, RSM UK Consulting LLP and Baker Tilly Creditor Services LLP are limited liability partnerships registered in England and Wales, with registered numbers OC325347, OC402439, OC325349, OC389499, OC325348, OC325350, OC397475 and OC390886 respectively. RSM Employer Services Limited, RSM UK Tax and Accounting Limited and RSM UK Management Limited are registered in England and Wales with numbers 6463594, 6677561 and 3077999 respectively. RSM Northern Ireland (UK) Limited is registered in Northern Ireland at Number One Lanyon Quay, Belfast, BT1 3LG with number NI642821. All other limited companies and limited liability partnerships are registered at 6th Floor, 25 Farringdon Street, London, EC4A 4AB. The UK group of companies and LLPs trading as RSM is a member of the RSM network. RSM is the trading name used by the members of the RSM network. Each member of the RSM network is an independent accounting and consulting firm which practises in its own right. The RSM network is not itself a separate legal entity in any jurisdiction. RSM Legal LLP is authorised and regulated by the Solicitors Regulation Authority, reference number 626317.

XPS Administration Limited
Engagement Letter



SCOPE OF THE REPORTING ACCOUNTANTS' WORK

We conduct our work in accordance with the procedures set out in AAF 01/20, issued by ICAEW. Our work will include enquiries of management, together with tests of certain specific control activities.

In reaching our conclusion, the criteria against which the control activities are to be evaluated are the internal control objectives developed for service organisations as set out within the AAF 01/20 issued by ICAEW.

Any work already performed in connection with this engagement before the date of this letter will also be governed by the terms and conditions of this letter.

We may seek written representations from Senior Management in relation to matters on which independent corroboration is not available. We shall seek confirmation from Senior Management that any significant matters of which we should be aware have been brought to our attention.

This engagement is separate from, and unrelated to, our audit work on the financial statements of the Service Organisation for the purposes of the Companies Act 2006 or other legislation and nothing herein creates obligations or liabilities regarding our statutory audit work, which would not otherwise exist.

INHERENT LIMITATIONS

Senior Management acknowledge that control activities designed to address specified control objectives are subject to inherent limitations and, accordingly, errors or irregularities may occur and not be detected. Control activities cannot guarantee protection against fraudulent collusion especially on the part of those holding positions of authority or trust. Furthermore, the opinion set out in the Service Auditors Report will be based on historical information and the projection of any information or conclusions in the Service Auditor's Report to any future periods will be inappropriate.

USE OF THE SERVICE AUDITORS REPORT

The Service Auditor's Report will, subject to the permitted disclosures set out in this letter, be made solely for the use of Senior Management of the Service Organisation, and solely for the purpose of reporting on the internal controls of the Service Organisation, in accordance with these terms of our engagement.

Our work will be undertaken so that we might report to Senior Management those matters that we have agreed to state to them in the Service Auditor's Report and for no other purpose.

The Service Auditor's Report will be issued on the basis that it must not be recited or referred to or disclosed, in whole or in part, in any other document or to any other party, without the express prior written permission of the Service Auditor. We permit the disclosure of the Service Auditor's Report, in full only, to User Entities of the Service Organisation using the Service Organisation's pension administration services ('User Entities'), and to the auditors of such User Entities, to enable User Entities and their auditors to verify that the Service Auditor's Report has been commissioned by Senior Management of the Service Organisation and issued in connection with the internal controls of the Service Organisation without assuming or accepting any responsibility or liability to them on our part.

To the fullest extent permitted by law, we do not and will not accept or assume responsibility to anyone other than Senior Management as a body and the Service Organisation for our work, for the Service Auditor's Report or for the opinions we will have formed.

We will, exceptionally, agree to permit the disclosure of the Service Auditor's Report on the Service Organisation's website, subject to, prior to this, us agreeing with you the wording of the introduction to the Service Auditor's Report (Appendix 2) within the service organisation controls report and on your website. In addition this permission is granted only if the Service Auditor's Report is published in full, to customers and potential customers of the Service Organisation using the Service Organisation's services ('User Entities') and to the auditors of such User Entities, to enable User Entities and their auditors to verify that the Service Auditor's Report has been commissioned by Senior Management of the Service Organisation and issued in connection with the internal controls of the Service Organisation without assuming or accepting any responsibility or liability to them on our part.

The Service Auditor's Report must not be relied upon by User Entities, their auditors or any other third party (together 'Third Parties') for any purpose whatsoever. RSM Risk Assurance Services LLP (the 'Service Auditor') neither owes nor accepts any duty to Third Parties and shall not be liable for any loss, damage or expense of whatsoever nature which is caused by their reliance on our Report. Should any Third Party choose to rely on the Service Auditor's Report, they will do so at their own risk.

**XPS Administration Limited
Engagement Letter**



The Service Auditor's Report must not be recited or referred to in whole or in part in any other document and must not be made available, copied or recited to any Third Party without our express written permission.

TERMS AND CONDITIONS OF BUSINESS AND ADDITIONAL TERMS

Our Terms and Conditions of Business form part of this Engagement Letter. They include certain of the definitions used in this letter. Please read carefully these Terms and Conditions of Business, which apply to all our work, as they include various exclusions and limitations on our liability, save where amended below.

It is agreed that, in relation to this engagement, the following clause shall be added

'5.13 To the fullest extent permitted by law, the Organisation agrees to indemnify and hold harmless RSM Risk Assurance Services LLP and its partners and staff against all actions, proceedings and claims brought or threatened against RSM Risk Assurance Services LLP or against any of its partners and staff by any persons other than the Directors as a body and the Organisation, and all loss, damage and expense (including legal expenses) relating thereto, where any such action, proceeding or claim in any way relates to or concerns or is connected with any of RSM Risk Assurance Services LLP's work under this engagement letter.'

AGREEMENT OF TERMS

We shall be grateful if you will confirm in writing your agreement to these terms by signing and returning the enclosed copy of this letter or let us know if the services covered are not in accordance with your understanding of the assignment to be carried out under the terms of this engagement.

For the avoidance of doubt, the terms covered by the Engagement Letter shall take effect upon receipt by us of your written agreement to them, or upon commencement of the work to which they relate, whichever is the sooner.

Yours faithfully

RSM Risk Assurance Services LLP

RSM RISK ASSURANCE SERVICES LLP

Encs. Terms and Conditions of Business dated May 2018

Contents noted and agreed for and on behalf of XPS Administration Limited

Signed 
AUTHORISED SIGNATORY

Date 27th May 2021



About us

XPS Pensions Group is the largest pure pensions consultancy in the UK, specialising in actuarial, covenant, investment consulting and administration. The XPS Pensions Group business combines expertise, insight and technology to address the needs of over 1,000 pension schemes and their sponsoring employers on an ongoing and project basis. We undertake pensions administration for over 930,000 members and provide advisory services to schemes of all sizes including 25 with over £1bn of assets.

Contact us

xpsgroup.com

Belfast

T: 028 9032 8282

1st Floor – Flax House
83-91 Adelaide Street
Belfast
BT2 8FF

Birmingham

T: 0121 230 1900

1 Colmore Row
Birmingham
B3 2BJ

Bristol

T: 0117 202 0400

33 – 35 Queen Square
Bristol
BS1 4LU

Bristol

T: 0117 369 3663

Cote House
The Promenade
Clifton, Bristol
BS8 3NG

Chelmsford

T: 01245 673 500

Priory Place
New London Road
Chelmsford
CM2 0PP

Edinburgh

T: 0131 370 2600

3rd Floor – West Wing
40 Torphichen Street
Edinburgh
EH3 8JB

Guildford

T: 01483 330 100

Tempus Court
Onslow Street
Guildford
GU1 4SS

Leeds

T: 0113 244 0200

1 City Square
Leeds
LS1 2ES

London

T: 020 3967 3895

11 Strand
London
WC2N 5HR

Please direct all email enquiries to:

E: enquiries@xpsgroup.com

Manchester

T: 0161 393 6860

10th Floor Chancery Place
50 Brown Street
Manchester
M2 2JG

Middlesbrough

T: 01642 727331

Vancouver House
Gurney Street
Middlesbrough
TS1 1JL

Newcastle

T: 0191 341 0660

4th Floor – Wellbar Central
Gallowgate
Newcastle
NE1 4TD

Perth

T: 01738 503 400

Saltire House
3 Whitefriars Crescent
Perth
PH2 0PA

Portsmouth

T: 023 94 31 11 66

One Port Way
Port Solent
Portsmouth
PO6 4TY

Reading

T: 0118 918 5000

Phoenix House
1 Station Hill
Reading
RG1 1NB

Stirling

T: 01786 237 042

Scotia House
Castle Business Park
Stirling
FK9 4TZ

Wokingham

T: 0118 313 0700

Albion
Fishponds Road
Wokingham
RG41 2QE

Award winning

PROFESSIONAL
PENSIONS
UK PENSIONS
AWARDS 2021

WINNER

Investment Consultancy
of the Year
XPS Pensions Group

PROFESSIONAL
PENSIONS
UK PENSIONS
AWARDS 2021

WINNER

Actuarial/Pensions Consultancy
of the Year
XPS Pensions Group

PROFESSIONAL
PENSIONS
UK PENSIONS
AWARDS 2021

HIGHLY COMMENDED

Third-Party Administrator
of the Year
XPS Pensions Group

PROFESSIONAL
PENSIONS
UK PENSIONS
AWARDS 2021

HIGHLY COMMENDED

Educational and Thought
Leadership Initiative of the Year
XPS Pensions Group

PROFESSIONAL
PENSIONS
UK PENSIONS
AWARDS 2020

WINNER

Third-Party Administrator
of the Year
XPS Pensions Group

PROFESSIONAL
PENSIONS
UK PENSIONS
AWARDS 2019

WINNER

Third Party Administrator
of the Year

PROFESSIONAL
PENSIONS
UK PENSIONS
AWARDS 2019

WINNER

Actuarial/Pensions
Consultancy of the Year



© XPS Pensions Group 2022. XPS Pensions Consulting Limited, Registered No. 2459442. XPS Investment Limited, Registered No. 6242672. XPS Pensions Limited, Registered No. 03842603. XPS Administration Limited, Registered No. 9428346. XPS Pensions (RL) Limited, Registered No. 5817049. XPS Pensions (Trigon) Limited, Registered No. 12085392.

All registered at: Phoenix House, 1 Station Hill, Reading RG1 1NB.

XPS Investment Limited is authorised and regulated by the Financial Conduct Authority for investment and general insurance business (FCA Register No. 528774).

This report should not be relied upon for detailed advice. Permission for reproduction of material in this document must be sought in advance of any public domain use.