PENSION ADMINISTRATION

Assurance Report on Internal Controls

AAF 01/20 and ISAE 3402

Report for the period 1 April 2022 to 31 March 2023

BARNETT WADDINGHAM

beyond the expected

Contents

Introduction to the AAF report

AAF 01/20 reporting

Barnett Waddingham is pleased to present this assurance report which describes the control environment within our Pension Administration Business Area. The report is based upon the framework for pension administration services as set out in the Technical Release 01/20 AAF "Assurance Reports on Internal Controls of service organisations made available to third parties" issued by the Audit and Assurance Faculty of the Institute of Chartered Accountants in England and Wales. This is consistent with ISAE 3402 "Assurance Reports on Controls at a Service Organisation" issued by the International Auditing and Assurance Standards Board. We have therefore adopted a dual reporting approach under both AAF 01/20 and ISAE 3402, however, the report will be referred to as an AAF 01/20 report. There have been no other changes to the regulatory environment.

We believe this report demonstrates the very highest standards of reporting across the industry covering each of our nine offices and all aspects of our pension administration service. This report covers the period from 1 April 2022 to 31 March 2023 and contains an independent opinion on the operating effectiveness, as well as the existence and effectiveness of design, of our control procedures.

"As our world becomes ever more digitised, the need for robust data security is greater than ever. Our commitment to managing and holding client information comes without compromise. This report, along with our Pensions Administration Standards Association (PASA) accreditation, our Gold Standard award for Investors in Customers, our Cyber Essentials and Cyber Essentials Plus certifications, and our ISO27001 and ISO9001 certifications, helps to prove we are a trusted partner for our clients."

PAUL LATIMER
Partner and Head of Pension Administration – Barnett Waddingham

Our Pension Administration internal controls team

Head of Pension Administration, Paul Latimer, has overall responsibility for procedures and internal controls. Richard Goddard, Senior Internal Controls and Quality Audit Manager, is responsible for maintaining the control environment within our Pension Administration Business Area and oversees the annual independent audit of the design and operating effectiveness of our internal controls.

A team of experienced pension administrators, consisting of Philippa Wardman, Chris Flanagan and Charlie Farrell supported this year's audit.

If you have any questions, or wish to discuss the content of the report, please contact Paul Latimer on 01494 788134 or Richard Goddard on 01242 548590.

Report statistics

The AAF 01/20 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 Barnett Waddingham's pension administration services' internal controls but are not a reliable measure for comparison.

Risk area	Control Objectives	Control Activities	Exception count
Pension Administration			
Accepting clients	3	8	0
Authorising and processing transactions	3	27	0
Maintaining financial and other records	4	22	0
Safeguarding assets	2	20	0
Managing and monitoring compliance and outsourcing	5	12	0
Reporting to clients	2	6	0
Information Technology			
Restricting access to systems and data	4	25	0
Maintaining integrity of the systems	5	20	0
Maintaining and developing systems hardware and software	3	8	0
Recovering from processing interruptions	5	13	0
Managing and monitoring compliance and outsourcing	2	4	0
TOTAL	**38**	**165**	**0**

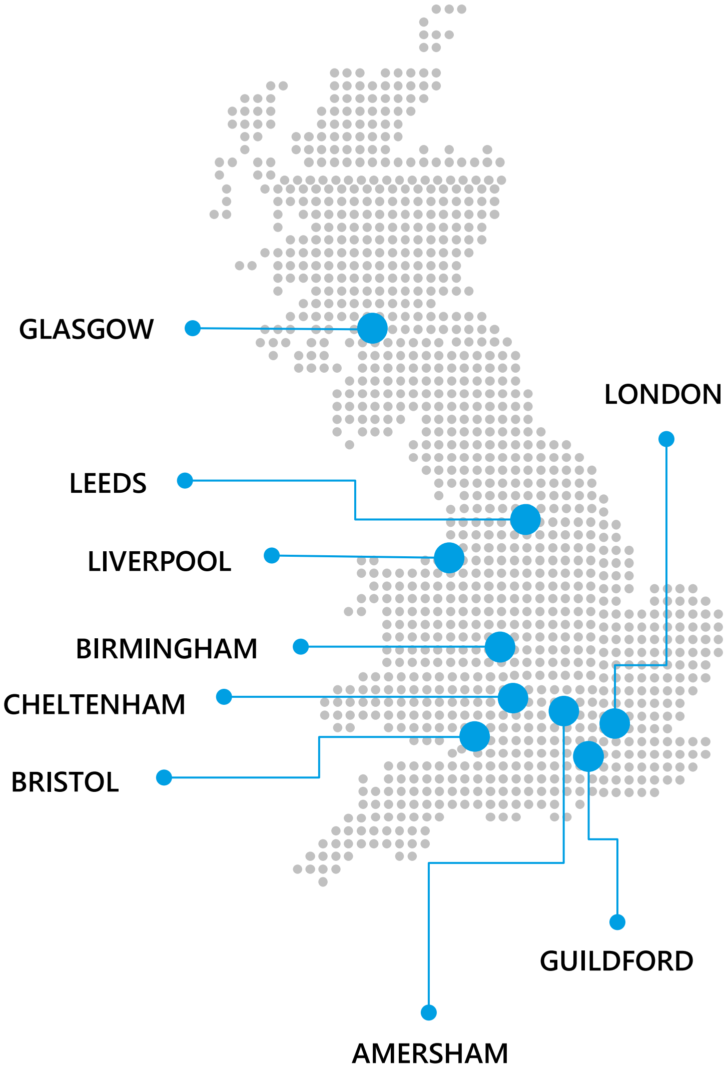
About us

We are proud to be a leading independent UK professional services consultancy at the forefront of risk, pensions, investment and insurance.

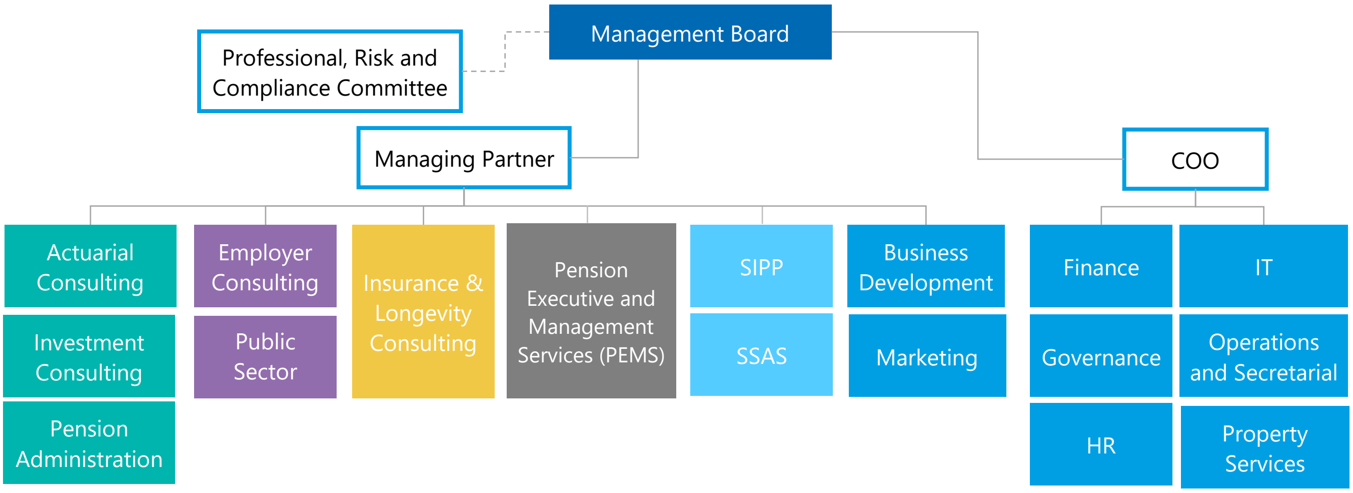
With a team of more than 1,500 people in nine offices, including 94 partners, we work to deliver on our values and our promise, ensuring the highest levels of trust, integrity and quality.

We act as a trusted partner for a wide range of clients in both the private and public sectors – this includes almost 25% of FTSE 100 and almost 15% of FTSE 350 companies.

We are free from any external stakeholders, allowing us to take a long-term view with all our clients and giving us the freedom to bring fresh ideas to the table, unobstructed.



The following diagram shows the operational structure of Barnett Waddingham for the company year commencing 1 June 2022:



Our guiding values

Our people are key to the success of our business and we are exceptionally proud of their loyalty and commitment to delivering a quality, efficient client service. People who join Barnett Waddingham tend to stay, thriving in a professional learning environment and caring, friendly culture.

Our values drive how our people act and are the embodiment of our promise – to do the right thing. These values help guide us and bring us together as one team. We've distilled this down to four statements which are embedded across the entire business.

Principled

We are committed to maintaining our high ethical standards whilst considering the impacts on all our stakeholders. We behave in a manner that demonstrates our honesty, conviction, pride and responsibility to keep our promises. We continue to uphold our reputation as an independent partnership that has integrity at its core.

Quality

We don’t compromise on quality; excellence is the norm across our whole business and we consciously look to provide innovative solutions that deliver ongoing value to every client.

Partnership

By working collaboratively within the firm and with our clients, we are able to deliver a seamless service by encouraging both individual excellence and teamwork within our business. Our unified approach ensures we are working together toward the same goals and desired outcomes.

Respect

We recognise and respect the value of everyone’s contribution to our success, honouring our diversity and the positive effect we have on our communities and the environment.

An award-winning team

Our success is built on rigorous commitment to client service, unique expertise and a culture of innovation.

Operating in highly competitive markets, our long list of achievements would mean little if they did not stand up to independent scrutiny. Our efforts are consistently recognised by some of the most influential organisations in the industry.

Pensions expert
PENSION AND INVESTMENT PROVIDER AWARDS 2022
Winner
THIRD-PARTY ADMINISTRATOR OF THE YEAR
Barnett Waddingham

corporate adviser awards 22
WINNER
BEST PENSION ADVISER
WINNER
BEST ESG BENEFITS CONSULTANT
WINNER
CORPORATE ADVISER FIRM OF THE YEAR

THE UK HEALTH+PROTECTION AWARDS 2022
in association with Allianz Partners
WINNER
Best Workplace Wellbeing Advice Firm

Pension Administration

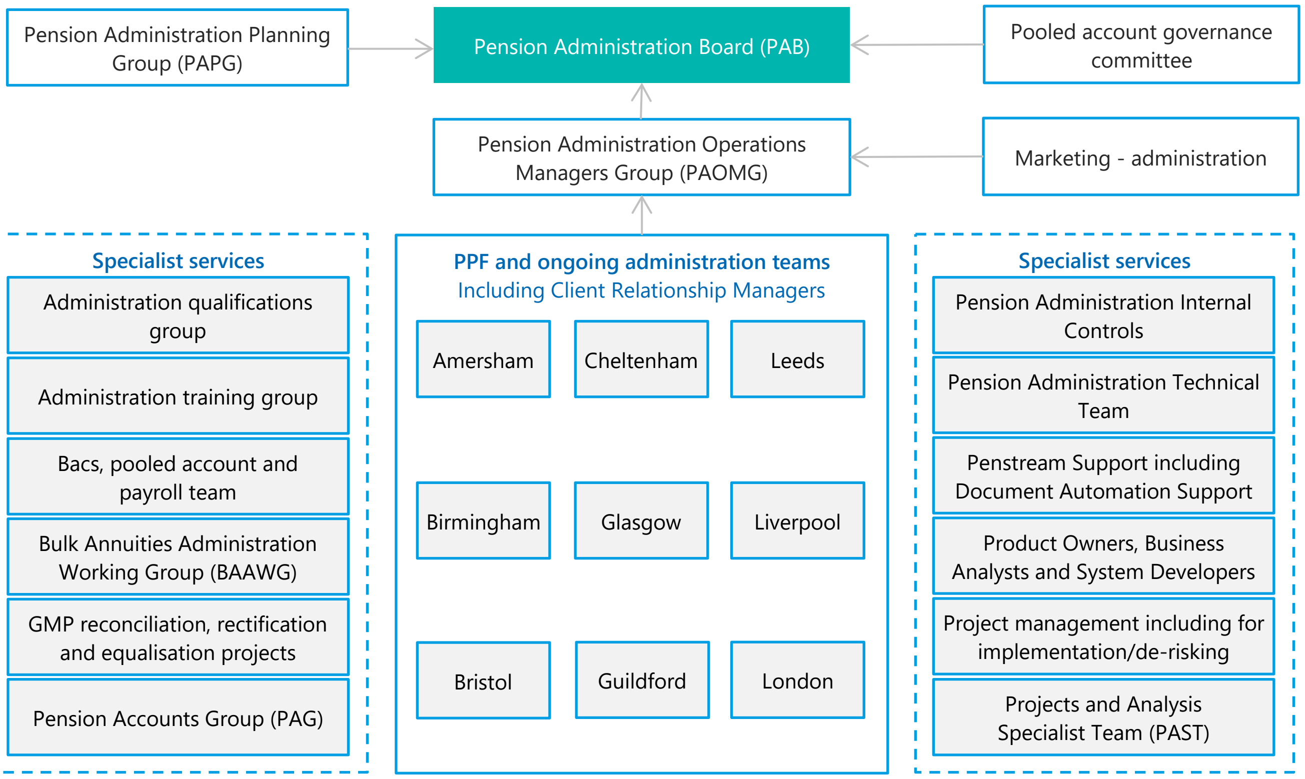
Our experienced and professional pension administration team provides services to over 400 clients including schemes comprising 40,000 members; covering defined contribution, defined benefit, hybrid, Career Average Related Earnings (CARE), open, closed and those transferring to the Pension Protection Fund (PPF).

Our team includes over 500 specialist pension administrators who have over 2,500 years of relevant pensions administration work experience between them.

We provide the full range of pension administration services which includes:

- membership record keeping;
- benefit calculations and payments including electronic payments;
- all regulatory reporting including eFiling;
- full cash and accounting services including drafting the annual report and accounts and pooled banking facilities;
- pensioner payroll;
- data audits and data cleansing exercises, particularly where data originates from multiple sources;
- internet functionality and links to other systems (such as HM Revenue & Customs, Straight-through processing);
- GMP reconciliation exercises;
- de-risking project exercises; and
- specialist PPF services.

The following diagram shows the operational structure of the Pension Administration Business Area during the reporting period:



Pension Administration Planning Group (PAPG)

Pension Administration Board (PAB)

Pooled account governance committee

Pension Administration Operations Managers Group (PAOMG)

Marketing - administration

Specialist services

Administration qualifications group

Administration training group

Bacs, pooled account and payroll team

Bulk Annuities Administration Working Group (BAAWG)

GMP reconciliation, rectification and equalisation projects

Pension Accounts Group (PAG)

PPF and ongoing administration teams
Including Client Relationship Managers

Amersham

Cheltenham

Leeds

Birmingham

Glasgow

Liverpool

Bristol

Guildford

London

Specialist services

Pension Administration Internal Controls

Pension Administration Technical Team

Penstream Support including Document Automation Support

Product Owners, Business Analysts and System Developers

Project management including for implementation/de-risking

Projects and Analysis Specialist Team (PAST)

Pension Administration Board

For the company year beginning 1 June 2022, there were eleven partners within the Pension Administration Business Area. These partners report to Management Board through the Pension Administration Board (PAB). The PAB typically meet by way of video conferencing calls twice each week to decide high level priorities, targets and goals for the Pension Administration Business Area.

Two changes to PAB membership occurred during the reporting period. Shirley Jackson left the PAB and Sharon Khan joined, both effective from 1 June 2022.

Paul Latimer
Partner and Head of
Pension Administration

Nuala Hedges
Partner

Julian Mainwood
Partner

Sue Foley
Partner

Andy Greig
Partner

Chris Tagg
Partner

Ben Clacker
Partner

Fiona Rumsby
Partner

Amanda Bradley
Partner

Paula Hendry
Partner

Sharon Khan
Partner

Pension Administration Planning Group

The Pension Administration Planning Group (PAPG) includes all pension administration partners, principals and associates. Pension Administration specialist teams and relevant committees prepare and submit informational reports in advance of meetings which take place every four months. The PAPG consider and act upon any operational or business matters as directed by the PAB.

Pension Administration Operations Managers Group

The Pension Administration Operations Managers Group (PAOMG) comprises operations managers representing each of our nine offices. PAOMG recommend or have input on proposed operational changes, share and promote communications on operational matters and ensure Business Plan initiatives are implemented effectively and consistently. The operations managers act as line managers for the administration team leaders, and they evaluate priorities across the administration teams to ensure the delivery of an efficient service that meets with client expectations.

Pension administration teams

Our ongoing and PPF administration teams consist of pension administrators with a full range of experience and skills in order to provide an efficient and cost-effective service to our clients. A team leader manages each team's workload to ensure that all work is completed within the required timescales and that administrators with the appropriate expertise are available to check the work of less experienced administrators. Where necessary, teams may call upon the expertise of specialist support teams.

Specialist support

Alongside the pension administration teams there are a number of specialist staff who provide either local support or centralised firm wide support. By concentrating support resources in these specialist fields, we can focus our expertise where needed, enabling our pension administration teams to concentrate on the business of delivering quality administration to our clients.

Software

Penstream

Our proprietary administration system, Penstream, is used for day-to-day administration, record keeping, benefit calculations and processing of DB, DC and CARE pension data. It is fully integrated with Taskstream for workflow management and with Cashstream, which is used for all cash handling and accounting. Due to the integrated nature of our systems the pension payroll function is carried out within the Penstream system. We do not have to operate multiple systems, thus reducing the risk of error and inefficiencies.

Penstream is not an 'off-the-shelf' product. It has been developed in conjunction with our pension administration teams and is therefore designed to be fully flexible to meet the needs of both our clients and our pension administrators. Total integration of our administration system, cashflow and workflow management means we can deliver efficiency. This flexibility allows us to maximise automation and focus on value added administration, like communication with members.

Cashstream

Accounts and treasury are carried out using Penstream's cash handling module – Cashstream. Cashstream incorporates a cashflow reporting tool so that it can be seen how much money is in the trustee's bank account at any time and what is required for a future stream of payments.

Taskstream

Taskstream is our in-house workflow system. Taskstream is a project management, task management and time recording system with full workflow capabilities. All tasks, including those dealt with by our specialist teams, are logged and managed using Taskstream.

eFiling is our electronic data management and document imaging system. eFiling is integrated with Penstream, Taskstream and Member self-service to enable scanned images to be viewed alongside a member's Penstream record internally. We can also easily share documents with the trustee and members.

BWebstream registration portal

BWebstream is our secure, easy to use, fully integrated online registration portal for company pension schemes, giving exceptional control over administration. BWebstream registration then provides opportunities for online access at numerous levels to meet the user's particular needs, enabling them to find the right details anytime, anywhere, at the touch of a button.

For trustees, our online tools give a valuable insight into their scheme and – with everything online – saves precious meeting preparation time. This also lightens the load for HR and payroll teams by giving access to data, forms and reports as well as enabling files to be shared simply and securely.

Our Member self-service platform, accessed via the BWebstream registration portal, has been designed to allow members to access their personal information, view scheme documentation, prepare their own retirement projections, update their own contact details and request certain changes.

The upload documents functionality within the Member self-service platform allows members to send us their documents digitally. Members can verify their identity online too. This means they do not need to put any sensitive documents – such as passports and bank details – in the post, in keeping with our commitment to a safer and more efficient process.

penStream®

MAIN ADMINISTRATION PLATFORM

Day to day administration
Record keeping
Benefit calculations
Straight-through processing (STP)
Pensioner payroll
Processing of contributions

cashStream®

ACCOUNTING PACKAGE

Automatically records payments
Cash handling
Cash flow reporting
Automatically enforced transaction limits
Pooled account
Report & Accounts

taskStream®

WORKFLOW MANAGEMENT SYSTEM

Project management
Task management
Time recording
Link tasks to member records
Service level agreements
eChecklists

bwebStream®

SECURE ONLINE FACILITY FOR CLIENT ACCESS

Two-factor authentication | Real-time access to data | Scheme documents and governance | Penstream records
Secure file exchange | Auditor document access | Member self-service | Integration with actuarial tools

Fully integrated with each other and eFiling

> "Developing our own software means we can ensure our online tools always meets our clients' needs in the most efficient way."

PAUL LATIMER
Partner and Head of Pension Administration – Barnett Waddingham

PASA accreditation

The Pensions Administration Standards Association (PASA) was established to promote and improve the quality of pension administration services for UK pension schemes. Both The Pensions Regulator (TPR) and the Department for Work and Pensions (DWP) identify that good administration can be demonstrated by independent accreditation.

As an independent body which has raised standards in pension administration, PASA has re-accredited Barnett Waddingham for our commitment to best practice. Attaining PASA accreditation is the gold standard for high-quality pension administration.

> "This accreditation gives our clients the confidence we have the capability and experience to support them to the highest standard."
>
> **PAUL LATIMER**
> **Partner and Head of Pensions Administration**

PMI Insight Partner

Barnett Waddingham continues to support the Pensions Management Institute (PMI) as Administration Insight Partner, working with the PMI to provide the industry with a platform to access the most up to date, specialist information on pension administration.

In addition to technical and administration focused articles there are direct links to Barnett Waddingham's PATHways bulletins. These are produced by our Pension Administration Technical Help (PATH) team to keep pension administrators abreast of the latest hot topics impacting pension administration. These bulletins can also be found on our website at www.barnett-waddingham.co.uk/comment-insight/briefings/.

Future developments

Key to Barnett Waddingham's continuing success is our drive for continuous improvement in the quality and efficiency of our work. We use in-house software developed specifically for our requirements to ensure clients' needs are met in the most efficient way. Technology enhancements will increase efficiencies in processing without compromising the current quality level of our service, allowing our valuable staff to concentrate on the communication and consultancy aspects of their work.

During the next year we are working on:

- planning and development of the changes needed to support our clients with their Pensions Dashboards responsibilities, ensuring that we can fulfil all the regulatory requirements placed on schemes;
- continuing rollout and development of Insight, our online dashboard for trustees, which provides membership statistics and service level reporting; and
- improvements to Member self-service including introduction of a dashboard and case tracker functionality.

Control environment

Barnett Waddingham's aim is to maintain a controlled environment which ensures accuracy and timeliness of work and the protection of clients' assets, whilst providing sufficient flexibility at the appropriate level of seniority to meet any specific client needs. This strong control environment is achieved in many different ways.

Procedural guidance and eChecklists

Procedural guidance is an intranet-based manual of pension administration procedures for all controlled tasks which also holds technical information for pension administrators. It forms a key part of the quality procedures of the Pension Administration Business Area along with eChecklists which are used to guide administrators through controlled processes. Procedural guidance and eChecklists covering administration processes are maintained by the Pension Administration Technical Team who consider all suggestions and implement any appropriate changes referring to the PAB where necessary.

Communications

Pension Administrations' Document Automation Support Team is responsible for establishing and maintaining standard document templates for use by pension administrators. They liaise with other specialist groups within the firm, such as the Pension Administration Technical Team, to ensure document templates comply with regulatory requirements.

Standard member correspondence is generated for pension administrators by an automated process within Penstream which delivers member specific data and the results of calculations directly to a document template.

Review

Quality of work is paramount and our aim is to get everything right first time. Work is checked for reasonableness and accuracy by individuals with the appropriate experience and expertise.

Information security programme

ISO certification

Barnett Waddingham is proud to hold Quality Management (ISO 9001:2015) and Information Security Management (ISO 27001:2013) accreditations. ISO international standards ensure that products and services are safe, reliable and of good quality. For businesses, they are strategic tools that reduce costs by minimizing waste and errors, and increasing productivity.

One of the strengths of ISO standards is that they are created by the people that need them. Industry experts from over 160 countries drive all aspects of the standard development process, from deciding whether a new standard is needed to defining all the technical content. Both of our ISO certifications are based on the principle of continual improvement.

A business assesses its current situation, fixes objectives and develops policy, implements actions to meet these objectives and then measures the results. With this information the effectiveness of the policy and the actions taken to achieve it can be continually reviewed and improved. The adherence to these codes of practice is then demonstrated via independent auditing.

Barnett Waddingham first achieved ISO certification in 2013 and is committed to retaining it. Barnett Waddingham's Information Security Manager conducts regular internal audits to ensure compliance with controls is maintained.

Our ISO certificates can be viewed on our website at www.barnett-waddingham.co.uk/about-us/iso.

Cyber Essentials and Cyber Essentials Plus certified

The security of our information and that of our clients is paramount. Alongside our ISO certifications, Barnett Waddingham has continued its commitment to further improving information and data security by gaining both the Cyber Essentials certification and the Cyber Essentials Plus certification. Backed by the UK Government, Cyber Essentials standards are becoming a mandatory requirement for many businesses handling sensitive information at moderate to high-level risk.

Our Cyber Essentials and Cyber Essentials Plus certificates can be viewed on our website at www.barnett-waddingham.co.uk/about-us/iso.

Training

All new staff are required to complete cybersecurity and data protection training on their first day. A subsequent presentation is given to joiners as part of our national induction days.

Updates are shared with all partners and staff throughout the year including, for example, updates on the most common types of attacks they could be exposed to.

Our non-professional training programme covers a broad range of areas including cybersecurity and the regulatory environment - such as data protection, financial services and anti-money laundering procedures. There is a periodic refresher programme in place and an annual presentation is made available to the entire business covering reminders and updates on key policies and procedures. Refresher sessions can also be carried out on request.

An Information Security and Data Privacy Awareness programme is in place which provides regular updates, reminders and guidance on various topics including secure home working, use of social media, phishing and identity fraud and staying safe online. This programme is delivered via different mediums including eLearning modules, intranet blogs, email, presentations and corporate communication tools.

Policy reviews

Firmwide information security policies and procedures are subject to regular monitoring and annual reviews.

Personnel

Barnett Waddingham carry out comprehensive vetting of all individuals prior to employment. The identity of all staff and agents who will have access to confidential information is confirmed using verifiable identity documents prior to creating accounts which give access to confidential information.

Where any of these checks give cause for concern, a further investigation is carried out.

Physical security

Barnett Waddingham offices

Our offices are located in a mix of managed and self-managed properties. To ensure security is kept at our defined standards all office spaces are treated as self-managed, self-contained units independent of any extra security arrangements landlords may have.

We have implemented multi-layered security to safeguard access to our offices. This includes physical security controls including electronic access management, which ensures that only authorised employees, agents or sub-contractors can access the premises.

Further information relating to our office security measures can be found in the Controls section of this report under the Information Technology (Restricting Access to Systems and Data) heading.

Data centre

Where Barnett Waddingham hosts data using a third-party data centre, the hosting site has implemented multi-layered security to safeguard the data centre against unauthorised access 24 hours a day, 365 days a year. The comprehensive physical site security includes:

- onsite trained security staff 24/7;
- electronic access management;
- authorised access control list requiring a photo ID check to access data centre floor;
- locked server cabinets;
- 24/7 indoor and outdoor CCTV monitoring with video being saved for at least 30 days; and
- 24/7 physical intrusion monitoring alarm system.

All hosting facilities including buildings and infrastructure meet the standards set out in ISO/IEC 27001.

Follow me printing

Printing is only allowed to networked multi-function printer / copier devices and requires users to authenticate, using either an access card or a user ID and password, before they can collect any hard copy print-out. Locally attached printers are not supported.

Data protection and GDPR

Barnett Waddingham takes data protection very seriously and we adhere to the UK GDPR and Data Protection Act 2018. All partners and staff are required to follow the principles contained within the legislation.

To assist in achieving compliance with data protection principles, the partners of Barnett Waddingham LLP have:

- a Professional, Risk and Compliance Committee (PRCC) which acts as the focal point for risk management in Barnett Waddingham, and for overseeing compliance to internal and external requirements;
- appointed a Data Protection Officer (DPO), whose contact details can be provided on request;
- approved a comprehensive Information Security Management System (ISMS) which is applicable to all partners, consultants and staff; and
- delegated day to day oversight of our adherence to the ISMS to Barnett Waddingham's Information Security Manager.

Data Controller and Data Processor

The Terms of Business appended to Barnett Waddingham engagement letters sets out the responsibilities of the client and Barnett Waddingham depending on which party is acting as the Data Controller, Data Processor or both.

Data access and segregation

Where practical, a separate database can be set up for each client with only approved staff having access to the data.

Data anonymisation and pseudonymisation

Depending on the services provided, the principles of anonymisation and / or pseudonymisation of data will be used. Wherever possible, data will be anonymised i.e. all data that can identify a data subject will be removed and aggregated data will be used to provide the contracted services.

Personal data can, in certain circumstances, be pseudonymised e.g. key-coded. This involves the use of a key or identifier in lieu of personal data e.g. system generated member number.

Data used in non-production environments is anonymized prior to use.

Access to information

Access to confidential information is limited to authorised individuals, based upon the principles of least privilege and segregation of duties which limit all users to the lowest permission levels that they can be assigned that do not prevent the individual from completing their necessary tasks. Account access is periodically reviewed and access rights changed as necessary when an individual changes role.

Access to our private cloud Office 365 environment is protected by Multi Factor Authentication.

User accounts are disabled after 30 days of inactivity and removed from all systems after 60 days. Partner and senior manager accounts are retained for up to 90 days before full removal.

Data encryption

Each client database is encrypted. This uses encryption technology that shall be no less effective than Microsoft SQL – Transparent Data Encryption ("SQL TDE"), using a 256-bit AES encryption algorithm, or such other encryption algorithm as may be agreed to ensure that the encryption used remains current and standard industry practice.

Key management

Our key management is based on an EKM provider architecture that enables us to protect data encryption keys by using an asymmetric key stored with an external cryptographic provider. This model adds an additional layer of security and separates the management of keys and data.

A copy of our encryption keys is held in escrow with a third-party.

Retention periods

Data retention policies regarding customer and/or supplier data are governed by law and commercial practices. Personal data is held for no longer than is necessary for the purposes for which the personal data is processed.

Destruction of obsolete documented information and data

All paper waste other than publicly available content, such as periodicals, is treated as confidential and is placed in appropriate recycling bins. The recycling bins are emptied regularly. A BS15713 certified secure shredding and recycling company is used for disposal and certificates of secure destruction are provided.

In accordance with the clear desk policy, documents not required cannot be left unlocked in the open areas of the office outside normal working hours.

When no longer required, electronic data stored on server disk drives, CDs, removable storage drives and imaging equipment is destroyed. This is achieved by physically removing the storage media and having it destroyed by CESG approved third parties who provide certificates of destruction. In circumstances where disks cannot be removed all information is securely wiped.

Data transfers

All confidential information when stored on portable devices and media and when transmitted over any non-secure communication channels (internet, email or wireless transmission) including remote connectivity is encrypted. Confidential information is encrypted when stored on network file servers at rest and in backups and archives. Passwords, encryption keys and any keying material is not stored with any associated data. Encryption algorithms are 256-bit AES or such other algorithms as may be agreed.

When transferring confidential information we recommend that clients use secure email, such as enforced Transport Layer Security (TLS 1.2). For transferring data files, our secure communication services should be used.

Secure File Exchange (SFX)

Secure File Exchange (SFX) is an online service for sending and receiving files securely via a BWebstream account. The transmission of files through this service is encrypted using AES 256 encryption. Files sent and received using SFX are virus scanned during the transmission process. Files are held on a secure server that is physically located within Barnett Waddingham's server estate.

Data transfers out of the UK/EEA

All client data held will remain in the UK or EEA. We only transfer data physically or allow remote access to the data on the written instructions of the trustees or client or the Data Controller. Any authorised transfer will require the data to be transferred via secure channels.

Email security

We utilise an email security gateway which scans all inbound and outbound email. The platform will quarantine or reject inbound emails from blacklisted domains, emails with attachments that could contain malware, phishing emails, SPAM, impersonation emails and emails where SPF (Sender Policy Framework), DMARC (Domain-based Message Authentication, Reporting and Conformance) and / or DKIM (Domain Keys Identified Mail) records are either missing or incorrect.All email is monitored.

Data leak prevention

Data leak prevention tools are implemented on the email gateway to track, monitor, report and stop inadvertent and malicious data leaks. Our solution scans all email attachments and identifies potential leaks using policies based on keywords, file hashes, pattern matching and dictionaries. Emails containing suspected leaks are blocked and quarantined for review. Further controls are in place to stop malicious email attachments and links from entering and leaving our systems. In certain circumstances, personal data may be sent by email. In these specific cases, it must be contained in a password protected attachment with the password being communicated by other means, e.g. via SMS or a telephone call.

Systems change management

We have a robust change management system in place such that all changes to code, configuration and hosting environments are documented and approved by the appropriate authority prior to release.

Code versioning, builds and releases are managed using the Microsoft Azure DevOps toolchains. Code changes are submitted through pull-requests, peer reviewed and subjected to automated tests before being integrated into our test environments. Routine releases to the live environment are automated, subject to the necessary approval. Changes are traceable back to requirements through Microsoft Azure DevOps and our integrated work management systems.

Further information relating to our systems change management processes can be found in the Controls section of this report under the Information technology (Maintaining and developing systems hardware and software) heading.

Quality assurance

Quality Assurance technicians are embedded in our development teams and involved from the start in refining work and agreeing acceptance criteria. Our Software QA Technicians promote best practice in areas of accessibility, usability, browser / device support and automation of user testing.

Security

The BWebstream registration portal is the front-door to our client-facing systems and is run by a dedicated team focused on data and application security. This gives us standardisation in key areas of security around authentication and authorisation including the sharing of code libraries. We use industry-vetted cryptographic libraries, platforms and protocols – particularly the standard Microsoft web stack - as a means of mitigating security risks.

Device security

Build standards

Our servers and laptops are built using security tested standard images. We carry out regular vulnerability scans on our servers and implement security changes across the entire estate. We only enable services that are required and remove / change default passwords. Patches and hotfixes are applied when they are released by the vendor. We utilise Microsoft Group Policies to implement centralised security configuration controls across the network.

All clocks are synchronised to an external source.

Anti-malware

Personal computing devices (laptops, tablets and desktops) which connect to our corporate network have installed and enabled an endpoint security solution designed to stop malware, viruses and ransomware from infecting the machine and the network. Such endpoint protection software is a recognised enterprise security solution and includes Managed Detection and Response (MDR) functionality. To ensure complete protection we employ both signature based and signature less tools running in parallel. Updates to signature files are managed by our Mobile Device Management (MDM) application.

Device encryption

All corporate desktop and laptop PC's have full disk encryption turned on using industry standard enterprise device encryption technology.

Mobile devices

All corporate mobile devices including laptops, smartphones and tablets are enrolled in our Mobile Device Management (MDM) application. The MDM solution also provides full device encryption on smartphones and tablets. Full wipe or selective wipe functionality is available depending on device type.

In addition, all corporate mobile phones and tablets have an anti-malware, data backup and remote management application installed.

Security incident and event management

We have implemented a Security Incident and Event Management (SIEM) system which is monitored by an external Security Operations Centre (SOC) who are able to interpret and react to alerts raised by the system. Events requiring attention are reported to our IT Support team for action.

We have documented standard procedures for dealing with suspected and actual security events, incidents, breaches and cyber-attacks. All incidents are logged in a ticket management system.

Clients will be notified as soon as possible, and in any case within 24 hours of any suspected or actual security event, incident or cyber-attack which may have compromised any of the clients' confidential information in relation to its confidentiality, availability or integrity (as described in ISO 27001), irrespective of whether the data is known to have been ex-filtrated.

In the event of confidential information being compromised we will co-operate fully with clients in relation to investigation and remedial actions as may be required.

Business continuity

Back-up and recovery

For our hosted environment, a cloud-based backup solution is used. We perform daily, weekly, monthly, and yearly backups. All backups are encrypted and written to disk with yearly backups being stored for 7 years. Critical servers hosted in our primary data centres are replicated to our disaster recovery data centre using continuous replication technologies. Our Recovery Point Objective (RPO) for critical services is 15 minutes.

Back-up retention

Monthly snapshots of backup data are held for a rolling period of 12 months. The end of year snapshot is held for a minimum of 7 years.

Various backup data sets are tested on a monthly basis.

Business continuity and disaster recovery testing

Our business continuity plan and disaster recovery plan are tested at least once a year. Our Recovery Time Objectives (RTO's) are as follows:

- mission critical systems within three hours;
- business critical systems within six hours; and
- business desirable systems within nine to twelve hours.

Part of the recovery process testing is to ensure that systems are recoverable at a remote site and are accessible by members of staff from various business units. Any recommendations are followed up by our IT and Information Security Teams.

Statement by the Pension Administration Board of Partners

As Senior Management of Barnett Waddingham LLP ('the Service Organisation') we are responsible for the identification of Control Objectives relating to the provision of pension 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 User Entities 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 User Entities who have used the pension administration services and related information technology and their auditors who have a sufficient understanding to consider the description, along with other information including information about Control Activities operated by User Entities 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 pension administration and information technology 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 in the Controls section fairly presents the Service Organisation's pension administration services throughout the period 1 April 2022 to 31 March 2023. 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 User Entities' 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 User Entities' 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 User Entities and their auditors and may not, therefore, include every aspect of the services that each individual User Entity 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 April 2022 to 31 March 2023. 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.

We acknowledge that the Service Auditors were unable to perform any procedures over the following Control Objective:

- Data migration or modification is authorised, tested and, once performed, reconciled back to the source data.

We confirm that during the period 1 April 2022 to 31 March 2023 there were no qualifying activities performed that would demonstrate the Control Activity described in our report (7.27), which is the only Control Activity designed to meet the Control Objective described above.

Paul Latimer

Paul Latimer
Chairman, Pension Administration Board, Barnett Waddingham LLP
30 May 2023

Controls

Control Objectives

Accepting clients

- 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.

Authorising and processing transactions

- Contributions and transfers-in received, and where applicable allocation of members' funds to investment options 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.
- Switches of members' funds between investment options and other rebalancing transactions are processed completely, accurately and within agreed timescales.

Maintaining financial and other records

- 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.

Safeguarding assets

- Member records are securely held and access is restricted to authorised individuals.
- Cash in scheme bank accounts is safeguarded and payments are suitably authorised.

Managing and monitoring compliance and outsourcing

- Receipts of contributions are monitored against required timescales.
- Receipt of contributions, in accordance with schemes rules and legislative requirements, are monitored.
- 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 the standards set out in 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.

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

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 secure in line with external party agreements.
- Data received from external parties is scanned for known vulnerabilities, any compromised data is quarantined and definitions of threats are periodically updated.
- 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.
- Network perimeter security devices are installed and changes are tested and approved.

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

- The physical IT equipment is maintained in a controlled environment.
- In-scope systems and data are backed up and tested such that they can be restored completely and within agreed timescales.
- Performance and capacity of In-scope systems are monitored and issues are resolved.
- IT related Disaster Recovery Plans are documented, updated, approved and tested.
- 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.

Complementary user entity controls

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 within this report 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 Barnett Waddingham. 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.

Complementary User Entity Controls:

- Clients review the completeness and accuracy of data submitted to Barnett Waddingham.
- Clients communicate information to Barnett Waddingham in a timely manner.
- Clients have established authorisation protocols in place.
- Clients communicate access restrictions to add/delete/modify user account access for approved client contacts.
- Clients communicate changes to approved client contacts in a timely manner.

Subservice Organisations

Barnett Waddingham outsources some IT services and activities, as described in this report, to third party suppliers ("Subservice Organisations"). The Description has been prepared using the carve-out method of presentation for Subservice Organisations and only includes the Control Objectives and Control Activities of Barnett Waddingham. The Description does not extend to Control Activities of the Subservice Organisations.

Controls 7.35 and 7.36 describe how we monitor outsourced activities.

Accepting clients

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

Process description

New clients enter into a formal agreement, drawn up and agreed between Barnett Waddingham and the client. Barnett Waddingham maintain Engagement Terms templates which are controlled outside the Pension Administration Business Area by the Governance Team. Any changes to the standard templates are agreed by the administration partner after discussion with the Governance Team and/or legal advisers.

A formal Engagement Letter, which includes Terms of Business, is agreed by both parties before provision of services commences. The scope of pension administration services to be provided by Barnett Waddingham is outlined on one or more schedules put in place prior to commencing administration activity or as soon as possible thereafter.

Control activity	Auditor testing
1.01.1 - The partner in charge of the client signs the Engagement Letter signifying their approval of the Engagement Terms, including any client specific customisation.	**1.01.1** - For a sample of new clients, confirmed that the Partner in charge had signed the Engagement letter. No exceptions noted.
1.01.2 - The Engagement Letter is signed by an authorised representative of the client before provision of services commences.	**1.01.2** - For a sample of new clients, confirmed that Engagement Letter was signed by an authorised representative of the client before provision of services commenced. No exceptions noted.

Accepting clients

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

Process description

Identities of the client, trustees and employers are checked for validity using a range of data sources appropriate to the nature of the client's business.

Clients in a PPF assessment period will have been subject to a s120 notice from an insolvency practitioner or official receiver which triggers an information gathering process by the PPF. If a trustee has been appointed from the PPF panel no additional checks are carried out as this is sufficient to satisfy Anti-Money Laundering identity checking requirements.

Control activity	Auditor testing
1.02 - For non-PPF clients, an Anti-Money Laundering verification check is performed prior to pension administration services commencing. The review date and supporting information are recorded against the client record on Taskstream.	**1.02** - For a sample of new non-PPF clients, obtained the anti-money laundering verification check and confirmed that this had been completed, prior to pension administration services commencing, by a member of staff and retained on file. Confirmed that the review date and supporting information was recorded on Taskstream. No exceptions noted.

Accepting clients

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

Process description

To support the set-up of a new scheme on Penstream, the interpretation of the rules is recorded in a benefit specification document that is prepared for each client using the client's trust deed and rules.

For PPF clients the benefit specification is written by the appointer lawyers from the PPF panel.

Control activity	Auditor testing
1.03 - For non-PPF clients the benefit specification document is prepared under the supervision of the project manager and retained on the file, together with any validation correspondence with the client or their advisers.	**1.03** - For a sample of new non-PPF clients, confirmed that the benefit specification document had been prepared under the supervision of the project manager and was retained on the file. No exceptions noted.

Accepting clients

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

Process description

A designated project manager is appointed for the taking on of a new client. The project manager works with an implementation project team to ensure that all necessary steps are completed, including the notification to third parties, obtaining data and documentation from the outgoing service provider and setting up necessary signatory authorities and account facilities.

Services for PPF clients are subject to alternative bespoke project management frameworks designed and optimised for the specialist nature of this work and the differing requirements of each client.

Control activity	Auditor testing
1.04 - For non-PPF clients a new client service project template or new client service tasks with eChecklists are added to Taskstream and progress is reviewed by the project manager until the scheme implementation is complete. The project manager summarises the work performed and any outstanding items in an end of project report for the client.	**1.04** - For a sample of new non-PPF clients, through inspection, it was confirmed that a new client service project template or new client service tasks with eChecklist had been added to Taskstream and that these had been marked as completed by the Project Manager. Confirmed that an end of project report was produced for the client. No exceptions noted.

Accepting clients

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

Process description

Administration, payroll and accounts data is loaded onto Penstream and checks are performed to reconcile the imported information against any available totals provided by the outgoing service provider. Any gaps in required information are referred to the client or their advisers for clarification.

Control activity	Auditor testing
1.05.1 - For non-PPF clients data imported to Penstream is reconciled by the implementation project team to the source data which is retained indefinitely.	**1.05.1** - For a sample of new non-PPF clients, obtained evidence of the data import reconciliations being performed by the implementation project team. No exceptions noted.
1.05.2 - For non-PPF clients the implementation project team record data reconciliation exceptions on the risk, action, issue and decision (RAID) log.	**1.05.2** - For a sample of new non-PPF clients and data reconciliation exceptions, confirmed that these were recorded in the risk, action, issue and decision (RAID) log. No exceptions noted.
1.05.3 - For non-PPF clients the risk, action, issue and decision (RAID) log is owned by the project manager who is responsible for its maintenance. Any decisions made or actions taken are recorded on the log and referred to the client or their advisers if necessary.	**1.05.3** - For a sample of new non-PPF clients, confirmed that the RAID log had been reviewed by the project manager, with any decisions and actions to be taken recorded. No exceptions noted.

Authorising and processing transactions

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

Process description

Contribution receipts as notified by the client at the point of payment are added to Cashstream either manually by the pension administrator or as an automatic function of other Penstream processes. Banking transaction reconciliations and checks performed on contributions received are covered under another control objective (see 3.10 and 5.03).

Internally administered DC contribution receipts are processed by the pension administrator by loading the relevant data to member records on Penstream. The system calculates the split of the contributions between investment funds or managers. The pension administrator arranges for the investment instruction and the funds to be transferred to the investment managers in accordance with service levels agreed with the trustees.

Control activity	Auditor testing
2.01.1 - Investment splits are checked and the totals for investment are reconciled against the total contribution amount reported by the client. Any discrepancies are investigated and resolved and the file is marked accordingly by the processor and reviewer.	**2.01.1** - For a sample of schemes, across a sample of months, confirmed that investment splits were checked and the totals for investment were reconciled against the total contribution amount reported by the client. Confirmed discrepancies were investigated and resolved by the administrator and that the file was marked accordingly by the processor and reviewer. No exceptions noted.
2.01.2 - A Contribution cycle eChecklist is used to record the completion of each step of the process and the file is marked accordingly by the processor and reviewer.	**2.01.2** - For a sample of DC schemes, across a sample of months, inspected the DC monthly contribution cycle eChecklist and confirmed each step of the process had been completed and that the file was marked accordingly by the processor and reviewer. No exceptions noted.

Authorising and processing transactions

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

Process description

Following confirmation of each DC investment transaction, the pension administrator checks the amounts invested and units purchased per fund against the instructions issued. Unit purchase details are loaded to Penstream and applied to individual member records. Unit allocation details are prepopulated from the STP transaction confirmation or in non-STP cases the pension administrator adds the transaction information manually.

Control activity	Auditor testing
2.02.1 - Confirmed unit purchases are checked against the instructions for consistency. The Penstream calculation automatically cross checks the unit price and fund amount against the number of units and any discrepancies are investigated. The file is marked accordingly by the processor and reviewer.	**2.02.1** - For a sample of schemes, confirmed units purchased were reconciled against the instruction for consistency. Confirmed that any discrepancies noted were investigated and that the file was marked accordingly by the processor and reviewer. No exceptions noted.
2.02.2 - Total unit holdings on Penstream are reconciled against the investment manager's records following each investment cycle. The file is marked accordingly by the processor and reviewer.	**2.02.2** - For a sample of schemes, confirmed total unit holdings on Penstream had been reconciled against the investment manager's records following each investment cycle. Confirmed the file was marked accordingly by the processor and reviewer. No exceptions noted.

Authorising and processing transactions

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

Process description

Applications to transfer in pension savings from other arrangements are logged onto Taskstream and the pension administrator checks all requirements have been received before investing pension funds, where applicable, and issuing a statement of transferred in benefits to the member. A transfer in implementation eChecklist is used and progress is monitored against agreed service levels by a nominated pension administrator or the Team Leader.

Control activity	Auditor testing
2.03 - A transfer-in implementation eChecklist is used to record the completion of each step of the process and the file is marked accordingly by the processor and reviewer.	**2.03** - For a sample of transfer-in implementations, confirmed the corresponding eChecklist was used to record the completion of each step of the process and that the file was marked accordingly by the processor and reviewer. No exceptions noted.

Authorising and processing transactions

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

Process description

Retirement illustrations (or provision of options for DC benefits) are sent to members in advance of their Normal Retirement Date (NRD). A report is run at least annually from Penstream records to identify any members attaining NRD during the coming period, and each case is added to Taskstream as a dormant task. The task will be automatically activated by Taskstream at an appropriate time. Taskstream tasks are monitored by a nominated pension administrator or the Team Leaders for progress and completion against agreed service standards and statutory timescale requirements.

Control activity	Auditor testing
2.04 - Dormant tasks are added to Taskstream as part of the forthcoming retirement process. A forthcoming retirements eChecklist is used to record the completion of each step of the process and the file is marked accordingly by the processor and reviewer.	**2.04** - For a sample of forthcoming retirement tasks, confirmed that the dormant tasks had been set up appropriately in Taskstream. Confirmed the forthcoming retirements eChecklist was used to record the completion of each step of the process and that file was marked accordingly by the processor and reviewer. No exceptions noted.

Authorising and processing transactions

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

Process description

Benefits on leaving, retiring or death are established using an automated system calculation on Penstream.

Any changes required to the calculation basis as a result of rule changes or calculation accuracy are referred by the pension administrator to a Pension Systems Analyst. Permission to update scheme setup configuration on Penstream is restricted to authorised users in UaG (see 7.10). Legislative changes affecting all schemes are managed at system level in conjunction with the developers (see 7.25).

Control activity	Auditor testing
2.05 - Penstream calculations used to establish member benefits are checked for reasonableness or accuracy. The file is marked accordingly by the processor and reviewer.	**2.05** - For a sample of benefit payments, confirmed that Penstream calculations had been checked for reasonableness and accuracy; and that the file was marked accordingly by the processor and reviewer. No exceptions noted.

Authorising and processing transactions

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

Process description

Where required, authorisation for distribution of discretionary benefits or provision of augmentations is obtained by the pension administrator from the client before payment is made.

Control activity	Auditor testing
2.06 - The pension administration team obtain authorisation from the parties appropriate to the circumstances. The file is marked accordingly by the processor and reviewer.	**2.06** - For a sample of discretionary benefits, confirmed that appropriate authorisation had been obtained prior to payments and that the file had been marked accordingly by the processor and reviewer. No exceptions noted.

Authorising and processing transactions

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

Process description

Where Barnett Waddingham provides treasury services, a payment request form is generated by the pension administrator for each individual payment transaction, with the transaction details being recorded on Cashstream (see 3.09).

For payments arranged through the client's bank, the transaction authorisation process is carried out using the payment request form.

For payments arranged through Barnett Waddingham's pooled account, the relevant payment transaction inputs to the CCM Browser are generated automatically by Cashstream. The transaction authorisation process is then carried out in the CCM Browser. Control of user registrations and authorisation levels is detailed in another control objective (see 7.06.3).

Control activity	Auditor testing
2.07.1 - For payments arranged through the client's bank, payment request forms are approved by two authorisers, one of whom may also check the form. Where the payment exceeds Barnett Waddingham mandate limits, additional approval for the payment is sought from the client.	**2.07.1** - For a sample of payments, obtained the payment request form and confirmed they had been subject to the appropriate level of authorisation, in accordance with signatory arrangements agreed with the client. Confirmed that, within the sample, no instances were identified where the payments exceeded the Barnett Waddingham mandate limits and therefore client approval was not sought. No exceptions noted.
2.07.2 - For pooled account payments below the pre-agreed limit, two authorisers approve payment transactions in the CCM browser. Where a transaction exceeds a threshold pre-agreed with the client, a third authorisation is required from a Gatekeeper.	**2.07.2** - For a sample of payments made from the pooled account, confirmed that they had been subject to the appropriate level of authorisation. The CCM browser was inspected to confirm that evidence of authorisation had been retained. Where a transaction exceeded the threshold pre-agreed with the client, confirmed a third authorisation was evidenced from a Gatekeeper. No exceptions noted.
2.07.3 - Where a pooled account transaction exceeds a threshold pre-agreed with the client, evidence of client payment approval is reviewed by a Gatekeeper prior to them recording their authorisation in the CCM browser.	**2.07.3** - For a sample of payments, the payment transaction within CCM was obtained and it was confirmed that each transaction had been reviewed and released by a Gatekeeper and evidence of this review and release had been recorded in CCM. No exceptions noted.

Authorising and processing transactions

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

Process description

Where Barnett Waddingham arranges or instigates a disinvestment of member or scheme funds, a disinvestment request form is prepared by the pension administrator. Where STP is in place, the disinvestment transaction instruction inputs on the STP system are generated automatically by Penstream. The transaction authorisation process is carried out using the disinvestment request form, except where STP is being used and the authorisation process is instead carried out on the STP system (see 3.11).

Control activity

2.08 - Disinvestment request forms are checked by a second pension administrator and approved by two authorisers, one of whom may also check the form. Where the disinvestment exceeds Barnett Waddingham mandate limits, additional approval for the payment is sought from the client and retained on the file.

Auditor testing

2.08 - For a sample of disinvestments, inspected the disinvestment request forms and confirmed these were checked by a second administrator and approved by two authorisers. Where the disinvestment exceeded Barnett Waddingham mandate limits, confirmed additional approval for the payment was sought from the client and retained on the file.

No exceptions noted.

Authorising and processing transactions

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

Process description

For DC schemes, the pension administrator uses Penstream to calculate the required unit disinvestments. The pension administrator arranges for the disinvestment instruction to be sent in accordance with service levels agreed with the trustees.

Following confirmation of each disinvestment transaction, unit transaction details are loaded to Penstream and applied to individual member records. Where STP is used the Penstream unit transaction details are prepopulated from the STP transaction confirmation or alternatively in non-STP cases the pension administrator adds the transaction information manually.

Control activity	Auditor testing
2.09.1 - Penstream calculations generating the disinvestment instruction are checked for accuracy with reference to the disinvestment requirements. The file is marked accordingly by the processor and reviewer.	**2.09.1** - For a sample of disinvestments, confirmed Penstream calculations were checked for accuracy with reference to the disinvestment requirements. Confirmed the file was marked accordingly by the processor and reviewer. No exceptions noted.
2.09.2 - Disinvested funds received are checked against the instructions for consistency. The Penstream calculation automatically cross checks the unit price and fund amount against the number of units and any discrepancies are investigated. The file is marked accordingly by the processor and reviewer.	**2.09.2** - For a sample of disinvestments, confirmed transactions were checked against the instruction for consistency. Confirmed that any discrepancies identified by Penstream were investigated. Confirmed the file was marked accordingly by the processor and reviewer. No exceptions noted.

Authorising and processing transactions

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

Process description

Payroll Administrators maintain a list of payroll clients which is used to record the timely receipt of payroll processing data and follow up late submissions with the pension administrators responsible. Every month a Payroll Administrator issues details to all offices of the payroll deadline dates for the forthcoming month.

Penstream prevents the pension administrator from posting new pensioner transactions to the payroll directly, without review. The pension administrator checks that the amounts of pension being paid are consistent with the pensioners’ benefit entitlements under the scheme rules.

System access controls for Bacs submission are covered under another control objective (see 7.11).

Control activity	Auditor testing
2.10.1 - Additions of new pensioners to a client’s payroll are processed by the pension administrator who suspends the transaction on Penstream and records the details separately for reconciliation purposes. A second pension administrator checks the new pensioner details for accuracy and posts the suspended transaction to Penstream. An eChecklist is used to record the completion of each step of the process and the file is marked accordingly by the processor and reviewer.	**2.10.1** - For a sample of new pensioners, inspected the corresponding eChecklist and confirmed completion of each step of the process had been completed and that file was marked accordingly by the processor and reviewer. No exceptions noted.
2.10.2 - Payroll runs for each client are reconciled for recorded changes against the previous payroll. The file is marked accordingly by the processor and reviewer.	**2.10.2** - For a sample of pension payroll runs, evidence was obtained to confirm that reconciliations had been performed and the files were marked by the processor and reviewer. No exceptions noted.
2.10.3 - For each payroll run the recorded pension entitlement is compared against the pension currently in payment and any material differences are investigated. The file is marked accordingly by the processor and reviewer.	**2.10.3** - For the sample of payroll payments tested in 2.10.2, it was verified that the pension entitlement checks had been completed. Confirmed that the file was marked accordingly by the processor and reviewer. No exceptions noted.
2.10.4 - Payroll and PAYE payment request forms are checked by a second pension administrator who may also be an authoriser. Transactions in the CCM browser must be part released by an authoriser.	**2.10.4** - For a sample of payroll and PAYE payments, evidence was obtained to confirm the corresponding payment request forms were checked by a second pension administrator. Transactions in the CCM browser were part released by an authoriser. No exceptions noted.

Authorising and processing transactions

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

Process description

Pension indexation calculations are completed by the pension administrator in accordance with the scheme rules, using Penstream. Confirmation is sought from the trustees regarding discretionary increases. A pension increase eChecklist is used to document the calculation and processing of the indexation.

Control activity	Auditor testing
2.11.1 - Penstream calculation output reports are spot checked for accuracy. Particular attention is paid to those retiring within the previous year for correct proportioning of indexation. The file is marked accordingly by the processor and reviewer.	**2.11.1** - For a sample of pension index calculations it was confirmed that the output reports were spot checked for accuracy. Confirmed that the file was marked accordingly by the processor and reviewer. No exceptions noted.
2.11.2 - Calculated indexation totals are recorded separately for payroll change reconciliation. Alternatively, for external payrolls, the calculated indexation information is passed to the responsible paying body. The file is marked accordingly by the processor and reviewer.	**2.11.2** - For the same sample as 2.11.1 it was confirmed that the calculated indexation totals had been recorded on the payroll reconciliation sheet. Confirmed that, within the sample, no instances were identified for external payrolls. Confirmed that the file was marked accordingly by the processor and reviewer. No exceptions noted.

Authorising and processing transactions

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

Process description

Transfer value quotations for DB schemes are calculated by the pension administrator using either Penstream or a spreadsheet. Unless simply automating a pre-set proforma, this will be compiled either by, or under the supervision of, the Scheme Actuary, or for schemes going through a bulk annuity transaction, the insurer's actuary. Where required by the actuary or client, calculations falling outside agreed parameters are referred to the Scheme Actuary/insurer for validation and agreement e.g. over a certain level, or of a certain benefit type/basis.

Alternatively, the pension administrator submits data to the Scheme Actuary/insurer or their actuarial assistant who prepares the calculation and returns the results to the pension administrator for issue. Transfer value quotations are issued in accordance with statutory requirements.

Control activity	Auditor testing
2.12.1 - For transfer values calculated using Penstream or a spreadsheet, outputs are checked for reasonability and calculations falling outside agreed parameters are referred to the Scheme Actuary/insurer for validation. A transfer out quotation eChecklist is used to record the completion of each step of the process and the file is marked accordingly by the processor and reviewer.	**2.12.1** - For a sample of transfer out tasks, confirmed the transfer value outputs calculated using Penstream or a spreadsheet, were checked for reasonability and calculations falling outside agreed parameters were referred to the Scheme Actuary/insurer for validation. Confirmed a transfer out quotation eChecklist was used to record the completion of each step of the process and the file was marked accordingly by the processor and reviewer. No exceptions noted.
2.12.2 - For transfer values prepared or validated by actuarial or insurer staff, the pension administrator obtains and checks that the calculation result has been properly authorised by the actuarial or insurer staff before issuing the quotation. A transfer out quotation eChecklist is used to record the completion of each step of the process and the file is marked accordingly by the processor and reviewer.	**2.12.2** - For a sample of transfer values prepared or validated by actuarial or insurer staff, confirmed the administrator checked that the calculation result had been properly authorised by the actuarial or insurer staff before issuing the quotation. Confirmed the transfer out quotation eChecklist was used to record the completion of each step of the process and the file was marked accordingly by the processor and reviewer. No exceptions noted.

Authorising and processing transactions

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

Process description

Procedural Guidance is a manual of pension administration procedures which also holds technical information for pension administrators. Pension administrators use Procedural Guidance and eChecklists to guide them through processes and relevant legislation. For processes covering the calculation of, or amendments to, benefits payable and transfer values, Procedural Guidance and eChecklists are maintained by the Pension Administration Technical Team who also review and consider changes to legislation.

Control activity	Auditor testing
2.13 - For processes covering the calculation of, or amendments to, benefits payable and transfer values, changes to Procedural Guidance and eChecklists are reviewed for technical and structural accuracy and the reviewer records their approval in the Procedural Help branch of the ticket system.	**2.13** - For a sample of changes made to Procedural Guidance or eChecklists, confirmed these had been reviewed for technical and structural accuracy. Confirmed that the reviewer recorded their approval in the Procedural Help branch of the ticket system. No exceptions noted.

Authorising and processing transactions

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

Process description

Investment switches are logged on Taskstream and progress is monitored against agreed service levels by a nominated pension administrator or the Team Leader. The pension administrator uses Penstream to calculate the required unit sales or purchases. Switch instructions are checked by a second pension administrator and approved by authorisers (see 2.07 and 2.08).

Confirmed unit transaction details are prepopulated from the STP transaction confirmation or in non-STP cases the administrator adds the transaction information manually.

Details of requested switch transactions are confirmed in writing to the member once the transaction is completed. Transaction summaries are also included on annual benefit statements and those members with online access may log in at any time to review their unit holdings.

Control activity	Auditor testing
2.14.1 - Penstream calculations generating the switch instruction are checked for accuracy with reference to the switch requirements. The file is marked accordingly by the processor and reviewer.	**2.14.1** - For a sample of DC switches, a copy of the task eChecklist was obtained to verify that the calculations had been checked to the switch requirements. Confirmed the file was marked accordingly by the processor and reviewer. No exceptions noted.
2.14.2 - A DC switch eChecklist is used to record the completion of each step of the process and the file is marked accordingly by the processor and reviewer.	**2.14.2** - For a sample of DC switches, confirmed a DC switch eChecklist was used to record the completion of each step of the process and that the file was marked accordingly by the processor and reviewer. No exceptions noted.
2.14.3 - Confirmed unit sales and purchases are checked against the instructions for consistency. The Penstream calculation automatically cross checks the unit price and fund amount against the number of units and any discrepancies are investigated. The file is marked accordingly by the processor and reviewer.	**2.14.3** - For a sample of switches, confirmed the units sales and purchases were checked against the instruction for consistency. Confirmed the file was marked accordingly by the processor and reviewer. No exceptions noted.
2.14.4 - Scheduled tasks are set up on Taskstream and set to activate in advance of scheduled switches. On completion of a scheduled switch, a check is performed to ensure the next scheduled switch task is in place and evidence of the check is recorded on the eChecklist.	**2.14.4** - For a sample of scheduled switches, confirmed that a scheduled task had been set up within Taskstream, as a reminder for the next switch date. Confirmed that evidence of check being performed, to ensure that the next scheduled switch task is in place, was documented on the eChecklist. No exceptions noted.

Maintaining financial and other records

Member records consist of up-to-date and accurate information

Process description

New joiners are added to Penstream by the pension administrator when they join a scheme, once details are submitted by the client.

Control activity	Auditor testing
3.01 - New joiners are reviewed against eligibility conditions, salary caps and other limitations or special terms and any outstanding requirements or anomalies are resolved by corresponding with the client. A New entrant eChecklist is used to record the completion of each step of the process and the file is marked accordingly by the processor and reviewer.	**3.01** - For a sample of new joiners, it was confirmed that the administrators checked the eligibility conditions, salary caps and other limitation or special terms. Confirmed that the a New entrant eChecklist was used to record the completion of each step and that the file was marked accordingly by the processor and reviewer. No exceptions noted.

Maintaining financial and other records

Member records consist of up-to-date and accurate information

Process description

Pension administrators keep active member data up to date by means of an annual data load from the client or at such other frequency as required by the client. A renewal eChecklist is used by the pension administrator. Benefit statements, including recorded salary and other data, are distributed to active members. Members may review their benefit statements and any resulting data queries are investigated and resolved by the pension administrator.

Control activity	Auditor testing
3.02.1 - Data submissions from the client are reviewed for reasonableness by the pension administration team and any anomalies are resolved by corresponding with the client.	**3.02.1** - For a sample of data submissions, confirmed that the pension administrator had reviewed the data submissions from the client for reasonableness and where applicable, resolved any anomalies through correspondence with the client. No exceptions noted.
3.02.2 - Penstream benefit calculation outputs are checked for accuracy or reasonableness by the pension administration team. The file is marked accordingly by the processor and reviewer.	**3.02.2** - For a sample of data submissions, confirmed that the Penstream benefit calculation outputs were checked for accuracy or reasonableness by the pension administration team. Confirmed the file was marked accordingly by the processor and reviewer. No exceptions noted.

Maintaining financial and other records

Member records consist of up-to-date and accurate information

Process description

The pension administrator uses a Penstream generated membership movement report to perform a membership reconciliation which is reported to the client as part of the administration report. Administration report frequency and content may vary (see 6.01).

Control activity	Auditor testing
3.03 - Membership reconciliation data is checked for reasonableness. The file is marked accordingly by the processor and reviewer prior to the information being reported to the client.	**3.03** - For a sample of administration reports, confirmed that the membership reconciliation data was checked for reasonableness. Confirmed that the file was marked accordingly by the processor and reviewer. No exceptions noted.

Maintaining financial and other records

Member records consist of up-to-date and accurate information

Process description

The pension administrator extracts member data from Penstream for valuation purposes on a triannual basis, or as otherwise requested by the Scheme Actuary. The data is reviewed by a pension administrator before being forwarded to an internal or external actuary, who conducts further logic and tolerance checks. The actuary reports any additional data requirements and data queries back to the pension administrator.

Control activity	Auditor testing
3.04 - Data checks for reasonableness or accuracy are performed on extracted valuation data by the pension administration team before it is sent to the actuary. The file is marked accordingly by the processor and reviewer.	**3.04** - For a sample of schemes, confirmed that the data checks for reasonableness or accuracy were performed on extracted valuation data by the pension administration team before sending to the actuary. Confirmed the file was marked accordingly by the processor and reviewer. No exceptions noted.

Maintaining financial and other records

Requests to change member records are validated for authenticity

Process description

The identity of members who contact Barnett Waddingham regarding their benefits and data, by telephone or in writing, is checked before data is amended.

Control activity	Auditor testing
3.05.1 - The identity of a member who telephones is verified by checking at least two specific personal data items against known values on record. Electronic phone notes on Penstream oblige the pension administrator to perform identity checks before being able to record the message information, which is logically enforced by the system. Completion of identity verification checks is recorded on the file.	**3.05.1** - Through observation of Penstream, confirmed that the administrator was required to verify at least two specific personal data items, for all telephone changes, prior to being able to record electronic phone notes. For a sample of telephone changes, confirmed completion of identity verification checks had been recorded on the file. No exceptions noted.
3.05.2 - Letters and emails received are checked for authenticity by signature check, or for correct identity by verifiable data items, before amending member records. Completion of identity verification checks is recorded by the pension administrator on the file.	**3.05.2** - For a sample of member contacts (letters and email), confirmed that the administrator had checked for authenticity by signature check, or the correct identity prior to processing the change. Confirmed completion of the checks had been recorded by the pension administrator and retained on the file. No exceptions noted.

Maintaining financial and other records

Requests to change member records are validated for authenticity

Process description

Pension administrators will process member data changes only from properly authorised third parties.

Control activity	Auditor testing
3.06 - A check that the necessary authority has been received, or that the third party is properly authorised, is performed before processing data change requests from third parties e.g. Bacs Payment Schemes Limited, Power of Attorney. Completion of the authorisation check is recorded by the pension administrator on the file.	**3.06** - For a sample of member data changes, confirmed that the administrator checked that the necessary authority had been received, or that the third party was appropriately authorised before amending data. Confirmed completion of authorisation checks was recorded by the pension administrator on the file. No exceptions noted.

Maintaining financial and other records

Requests to change member records are validated for authenticity

Process description

With the exception of fast track address updates and members using Member self-service online via the BWebstream registration portal, on receipt of an authorised change instruction, the pension administrator logs the task onto Taskstream, modifies the member record on Penstream, and logs the task off Taskstream on completion.

An acknowledgement is issued to the member confirming the modification except where notification is received direct from the client or is a technical amendment via Bacs. Where the modification is a change of address, and an acknowledgement letter is sent, it is issued to both the current and previous address, if known. Taskstream is monitored and progress against agreed service levels is reviewed by a nominated pension administrator or the Team Leader.

Address update notifications received by telephone may be processed by the pension administrator in real time during the call following a fast track process on Penstream. In these instances there is no eChecklist. The process, controls and checks are logically enforced by the system as part of the fast track updating process. The task is created automatically by the system on Taskstream.

Control activity	Auditor testing
3.07.1 - Modifications to member records, including fast track address updates, are reviewed for authority, completeness and accuracy by reference to the authorised instruction by a second pension administrator. The file is marked accordingly by the processor and reviewer.	**3.07.1** - For a sample of member record modifications, the member record was reviewed to confirm each update had been marked by the administrator and subject to review, by a second administrator, to confirm authority, completeness and accuracy. Confirmed the file was marked accordingly by the processor and reviewer. No exceptions noted.
3.07.2 - The fast track address update process on Penstream requires the verification of ID and authorisation of the third party to be confirmed on screen before the member record can be updated, which is logically enforced by the system.	**3.07.2** - Through observation of Penstream, confirmed that fast track address update system required the verification of ID and authorisation of the third party to be confirmed, prior to the member record being updated. No exceptions noted.
3.07.3 - Bank account change notifications from members are required to be instructed in writing, except for those made by the member using Member self-service online via the BWebstream registration portal. Penstream bank account records cannot be modified by a single pension administrator and require a second pension administrator to authorise and post the change to the system. An audit trail is retained of all changes made in Penstream.	**3.07.3** - For a sample of bank account change notifications, confirmed that each notification had been subject to processing and authorisation by two independent administrators, prior to the change being posted in Penstream. Confirmed through observation that the second administrator is unable to post the update, if they have edited the change. Confirmed audit trail of changes made in Penstream were retained. No exceptions noted.

Maintaining financial and other records

Requests to change member records are validated for authenticity

Process description

Members of schemes using Member self-service online via the BWebstream registration portal are able to access their records online and make basic changes to their records. Some changes require review by a pension administrator before the Penstream database is updated.

Granting members access to online records is described under another control objective (see 7.08.2).

Control activity	Auditor testing
3.08.1 - Requests to change member records, submitted online via Member self-service, are tested against validity parameters by Penstream before being posted to the database. Changes outside valid parameters are suspended and a Taskstream task is automatically created for a pension administrator to review and post the update to the member's record if appropriate, or follow up with the member.	**3.08.1** - For a sample of online member updates, confirmed that a Task ID had been created for updates outside of the parameters and updated by an administrator. No exceptions noted.
3.08.2 - Bank account changes submitted online by members are suspended on Penstream and a Taskstream task is automatically created for a pension administrator to review and post the update to the member's record if appropriate, or follow up with the member.	**3.08.2** - For a sample of bank account changes submitted online by members, confirmed these had been suspended on Penstream and that a Taskstream task was created for a pension administrator to review and post the update to the member's record. No exceptions noted.

Maintaining financial and other records

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

Process description

A benefit payment record is added to Cashstream automatically at the time of processing a transaction if it results from a function of Penstream processing. In other cases, the pension administrator enters the transaction details into Cashstream manually.

Where Barnett Waddingham provides treasury services using the client's bank, Cashstream transaction entry details are included on a payment request form.

Where treasury services are provided through Barnett Waddingham's pooled account, the relevant payment transaction inputs to the CCM Browser are generated automatically by Cashstream.

Control activity	Auditor testing
3.09.1 - The payment request form detailing the transaction is produced by the pension administrator and checked for completeness and accuracy by a second pension administrator. The file is marked accordingly by the processor and reviewer.	**3.09.1** - For a sample of payment requests, it was confirmed that the transaction was produced by the pension administrator and checked for completeness and accuracy by a second pension administrator. Confirmed the file was marked accordingly by the processor and reviewer. No exceptions noted.
3.09.2 - CCM browser transactions are created by Cashstream, the details of which are checked for reasonableness by the pension administrator and reviewed by a second pension administrator. The file is marked accordingly by the processor and reviewer.	**3.09.2** - For the same sample as 3.09.1, confirmed details of browser transactions were checked for reasonableness by the pension administrator and reviewed by a second pension administrator. Confirmed the file was marked accordingly by the processor and reviewer. No exceptions to note.

Maintaining financial and other records

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

Process description

Bank accounts are reconciled against Cashstream records at the appropriate frequency. The pension administrator cross checks all banking transactions between bank records and Cashstream for consistency.

For clients using their own bank account the receipt of a bank statement is logged onto Taskstream by the pension administrator and the statement reconciled against Cashstream records. Where required, regular transactions not subject to the payment request form process are posted to Cashstream during the reconciliation process. Taskstream tasks are monitored by a nominated pension administrator or the Team Leaders for progress and completion against agreed service standards.

Where treasury services are provided through Barnett Waddingham's pooled account the account is reconciled on a daily basis.

Control activity	Auditor testing
3.10.1 - Where Barnett Waddingham provides treasury services using the client's bank, Cashstream transactions are reconciled against the accounting system by the pension administration team each month following receipt of the bank statement. Any differences are investigated by the pension administration team and the reconciliation process continues until a cleared balance can be established on the accounting system equal to that on the bank statement. Cashstream retains records of all reconciliations.	**3.10.1** - For a sample of schemes, across a sample of months, confirmed that Cashstream transactions had been reconciled against the accounting system by the pension administration team following receipt of the bank statement. Inspected evidences to confirm any differences had been investigated and resolved. No exceptions noted.
3.10.2 - Where treasury services are provided through Barnett Waddingham's pooled account the pension administration team perform a daily reconciliation test between the bank account, CCM browser segregated account records and Cashstream. Any anomalies arising are investigated and resolved. Reports confirming the reconciliations are retained.	**3.10.2** - For a sample of days, obtained the daily reconciliation for the Barnett Waddingham pooled accounts and confirmed this had been completed by the pension administration team. Confirmed that any differences had been investigated and resolved. No exceptions noted.

Maintaining financial and other records

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

Process description

For DB schemes, monitoring of cashflow requirements is carried out by the administrator at monthly intervals or otherwise as agreed with the client.

Where STP is used the administrator records a required investment transaction on Cashstream which automatically generates the transaction instruction on the STP software or alternatively in non-STP cases the administrator manually prepares and issues the investment instructions subject to the authorisation requirements. The STP software logically enforces requirement for approvals at the correct levels (see 7.06.2).

An eChecklist is used by the administrator to record the investment or disinvestment process.

Control activity	Auditor testing
3.11.1 - Investment/disinvestment requirements identified from cashflow checks are reviewed for reasonableness and the file is marked accordingly by the processor and reviewer.	**3.11.1** - For a sample of investments/disinvestments, confirmed cashflow checks were reviewed for reasonableness and the file was marked accordingly by the processor and reviewer. No exceptions noted.
3.11.2 - An eChecklist is used to record the completion of each step of the investment/disinvestment process and the file is marked accordingly by the processor and reviewer.	**3.11.2** - For a sample of investment/disinvestment transactions, confirmed an eChecklist was used to record the completion of each step of the investment/disinvestment process and that file was marked accordingly by the processor and reviewer. No exceptions noted.
3.11.3 - STP transactions generated by calculations are checked and part approved by the pension administrator, and approved by a second authorised pension administrator prior to release. Alternatively, transactions are prepared by the pension administrator in accordance with the authorisation levels agreed with the client. The file is marked accordingly by the processor and reviewer.	**3.11.3** - For a sample of STP transactions generated by calculations, confirmed they had been checked and part approved by the pension administrator and fully approved by an authorised second pension administrator. Where manual calculation, confirmed transactions were prepared by the pension administrator in accordance with the authorisation levels agreed with the client. Confirmed the file was marked accordingly by the processor and reviewer. No exceptions noted.

Maintaining financial and other records

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

Process description

Investment records are maintained on Cashstream. Following confirmation of each investment transaction from the investment manager, the transaction details are checked, and for DB schemes using wholly invested unitised pooled funds, unit running totals are reconciled.

Control activity	Auditor testing
3.12 - For DB schemes using wholly invested unitised pooled funds, following receipt of the investment manager's transaction confirmation report, the unit running totals on the report are reconciled with those on Cashstream by the pension administration team and any differences are investigated and resolved.	**3.12** - For a sample of investment transactions, confirmed the unit running totals on Cashstream were reconciled by the pension administrator with those on the transaction confirmation report and any differences had been investigated and resolved. No exceptions noted.

Maintaining financial and other records

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

Process description

Other investment movements such as purchases and sales of assets, switches and swaps, derivatives, and changes in market value are updated on Cashstream as part of the periodic accounts preparation. An accounting period end eChecklist is used to record the completion of preparatory work on the accounts.

Control activity	Auditor testing
3.13 - On at least an annual basis, or for PPF schemes at least once during the PPF assessment period, investment manager reports are reviewed and the relevant transactions entered onto Cashstream by the pension administration team. On completion, the balances are reconciled to the period end investment reports and the transactions are recorded in the draft report and accounts document. The file is marked accordingly by the processor and reviewer prior to submission to external auditors.	**3.13** - For a sample of schemes, confirmed that the balances had been reconciled to the period end investment reports by the pension administrators, the reconciled amounts had been recorded in the draft report and accounts document. Confirmed the file was marked accordingly by the processor and reviewer prior to submission to external auditors. No exceptions noted.

Safeguarding assets

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

Process description

IT security policies and procedures are in place to prevent unauthorised access to electronic records (see section 7).

All electronic record keeping systems are password protected and have restricted access for authorised personnel only. The network password system is maintained by Network Administrators who normally receive instruction and authorisation for users from the Human Resources (HR) department. In special circumstances, a partner, principal or associate on the IT Committee may provide alternative authorisation.

Control activity	Auditor testing
4.01 - Network access rights for new users and leavers are maintained by following either the new starter or leaver process and actions are recorded on an eChecklist which is subject to review.	**4.01** - For a sample of new users and leavers, inspected the eChecklist and confirmed that new users and leavers process had been followed and actions had been recorded. Confirmed the eChecklist had been subject to review. No exceptions noted.

Safeguarding assets

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

Process description

Member and scheme files are held at Barnett Waddingham sites in paper, microfiche or electronic form, and in off-site storage facilities. Access to all office sites is controlled and described under a different control objective (see 7.01). Paper records retained in off-site storage facilities are managed by a single third party national supplier. Disaster recovery and data backup procedures are in place to minimise the impact of threats on client work and data storage. Details of software backup and disaster recovery controls are provided under a different control objective (see 7.30 and 7.32).

Waste paper produced by pension administration teams is disposed of in secure locked bins on site, which are emptied and maintained by a third party national supplier.

The new supplier process identifies third party suppliers who handle confidential material as Critical Suppliers. Contracts with Critical Suppliers are agreed only once the supplier is able to fully meet Barnett Waddingham's requirements from a legal, regulatory, environmental, sustainability and Cyber Security perspective.

Control activity	Auditor testing
4.02 - Critical Supplier contracts are approved by the Governance Team and the relationship is overseen by a partner. Only partners are authorised to sign contracts on behalf of Barnett Waddingham.	**4.02** - For a critical supplier with a new contract, confirmed that the contract had been approved by the Governance Team, and that this had been signed by a Partner. No exceptions noted.

Safeguarding assets

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

Process description

All letters and statements produced by Barnett Waddingham are retained indefinitely in electronic archives on the network and in the data backup systems. Access to the network and offsite backups are described under a different control objective (see 7.03 and 7.30). eFiling is our electronic data management and document imaging system which enables scanned images to be viewed alongside a member's Penstream record internally.

Control activity	Auditor testing
4.03 - The pension administrator eFiles letters and statements produced to the member record so that they are retained. All letters and statements are subject to review by a second pension administrator who records their approval of the letter/statement on the eFiling record.	**4.03** - For a sample of statements/letters sent to members, confirmed these had been eFiled, reviewed and approved by a second pension administrator, evidenced through the eFiling record. No exceptions noted.

Safeguarding assets

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

Process description

Personal member information transmitted electronically is protected from unauthorised access. Files are typically shared with clients and authorised third parties online using SFX (see 7.16.1). Alternatively, files are password protected prior to issue by email. The pension administrator copies all client emails to a shared client folder which is monitored for compliance with policy by other staff involved in that client’s work.

Control activity	Auditor testing
4.04.1 - Passwords must meet minimum specified complexity requirements as documented on the Password Policy, or as otherwise instructed by the client.	**4.04.1** - For a sample of emails containing attachments sent to scheme members, evidence was obtained to verify that the files were password protected, and that the password's were in line with BW's policy. No exceptions noted.
4.04.2 - Shared client email folders are periodically monitored by staff involved with, and the partner responsible for, the client. Breaches of email security policy which are identified as a result of monitoring are brought to the attention of Team Leaders and the individual concerned, either by email or verbally.	**4.04.2** - For a sample of logged email breaches, evidence was obtained to verify that the Team Leaders and individual concerned had been notified of the event. No exceptions noted.

Safeguarding assets

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

Process description

All employees are expected to comply with data protection legislation. The identity of members and third parties who contact Barnett Waddingham regarding member benefits and data, by telephone or in writing, is checked before data is released. Pension administrators release information only to properly authorised third parties.

Verifying the identity of telephone callers is described under another control objective (see 3.05).

Control activity	Auditor testing
4.05.1 - Letters and emails received are checked by the pension administrator for authenticity by signature check, or for correct identity by verifiable data items before outgoing written communication containing personal data is issued. Outgoing written communication is reviewed for completeness, accuracy, and adherence to the data protection policy by a second pension administrator who marks the file accordingly. Some short correspondence which has no figure work or content of substance, as determined by certain authorised administrators with the discretionary approval of their Team Leader, may be issued without review.	**4.05.1** - For a sample of outgoing written communications, evidence was obtained to verify that an authenticity check had been conducted, and the communication had been reviewed. Confirmed outgoing written communication was reviewed for completeness, accuracy, and adherence to the data protection policy by a second pension administrator. Confirmed the file was marked accordingly. No exceptions noted.
4.05.2 - The pension administrator checks that the necessary authority has been received from the client or member, that the third party is properly authorised, or that the disclosure is exempt under the UK GDPR or Schedules 2-4 of the Data Protection Act 2018, before releasing information to third parties. Outgoing communications are reviewed, and approval recorded on the file by a second pension administrator who checks that the appropriate authority has been received.	**4.05.2** - For a sample of third-party information requests, confirmed that the necessary authority from the client or member was obtained and reviewed to confirm it had been received prior to the information being released. Confirmed the outgoing communications were reviewed, and approval was recorded on the file by a second pension administrator who checked that the appropriate authority had been received. No exceptions noted.

Safeguarding assets

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

Process description

Member ID verification is required prior to benefit payments being made. Official documents (certificates, passports, driving licences) received by the pension administrator are promptly returned to the sender once ID verification checks have been performed.

Control activity	Auditor testing
4.06 - Original documents are returned in accordance with the guidelines held on the intranet. Normally Royal Mail Signed For or Special Delivery Guaranteed services are used according to the items being transported.	**4.06** - For a sample of tasks where original documents were provided to BW, confirmed that these were returned in accordance with guidelines held on the intranet. No exceptions noted.

Safeguarding assets

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

Process description

Each scheme has a separate bank account, except those with a segregated account within Barnett Waddingham's statutory trust pooled account arrangement. New scheme bank accounts are opened only by authorised personnel of the client.

Control activity	Auditor testing
4.07 - Creation of a new segregated pooled account record is required by the CCM Browser to be carried out by an authoriser and the system also requires authorisation by a Gatekeeper who checks that appropriate authorisation has been signed and received from the client.	**4.07** - For a sample of new segregated pooled account records, evidence was obtained to confirm the creation of a new segregated pooled account had been set up by an authoriser and authorisation from a gatekeeper had been obtained to confirm appropriate authorisation had been signed and received from the client. No exceptions noted.

Safeguarding assets

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

Process description

For clients using their own bank account facility, authorised signatory lists are maintained. Cheques and payment instructions requiring a signature are signed by authorised signatories. Pension administrators process all payment requests in accordance with the agreed signing limits.

Payment authorisation controls for clients using their own bank account facility and where treasury services are provided through the Barnett Waddingham pooled account are described under another control objective (see 2.07).

Control activity

4.08 - Amendments to the client signatory list are authorised by the client. Amendments to the Barnett Waddingham signatory list are authorised in accordance with the terms of the mandate put in place by the client which typically require two Barnett Waddingham partner, principal or associate signatories or a combination of client and Barnett Waddingham signatories.

Auditor testing

4.08 - For a sample of changes to the BW bank signatories, confirmed that these had been appropriately authorised by the client and in accordance with the terms of the mandate in place. No exceptions noted.

Safeguarding assets

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

Process description

On receipt of a new cheque book the pension administrator logs the task onto Taskstream and enters details of the book on either the office or pooled account cheque book inventory as appropriate. The pension administrator verifies that all cheques are present and that there is no evidence of tampering and logs the task off Taskstream on completion.

Control activity	Auditor testing
4.09 - Cheque book monitors appointed in each office routinely inspect the local cheque book safe/cabinet and inventory to confirm the process has been completed for all cheque books received during the period. Monitoring is performed every three months and the monitors findings are recorded on a monitoring task.	**4.09** - Confirmed monitoring task was performed by the cheque book monitors at least every three months at the BW sites, and that findings were recorded on a monitoring task. No exceptions noted.

Safeguarding assets

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

Process description

Cheque books and other payment devices are stored in secure safes or cabinets at each office which are locked every night. Local managers determine which staff to authorise for safe/cabinet access and distribute keys and combinations accordingly. To safeguard business continuity, nominated authorised individuals are permitted to hold payment devices outside our offices.

Control activity	Auditor testing
4.10 - Combination numbers for safes and cabinets are routinely changed at least every six months.	**4.10** - Confirmed that combination numbers for safes and cabinets had been changed at least every six months. No exceptions noted.

Safeguarding assets

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

Process description

Processing of electronic payments via the Bacs Bureau facility is carried out by authorised staff with either a Creator or Sender role. Payment entries on the Bacs processing system are checked by the Creator and authorised by the Sender. The system retains archives of all submitted payment requests.

Access to the Bacs processing system is limited to selected authorised staff and is password protected by network logon, access smartcard and PIN security (see 7.06.1).

Control activity

4.11 - The Creator processing the Bacs payment request checks for the presence of required payment authorisation before creating the payment request on the Bacs processing system. All Bacs Bureau payment requests are reviewed and checked for accuracy by a Sender who then submits the payment request to Bacs. Bacs submission summary reports, including a record of the Creator and Sender, are retained on the Bacs processing system.

Auditor testing

4.11 - For a sample of Bacs payments, transmission reports were obtained and reviewed to confirm that each report included evidence with respect to the creator and sender and the report had been retained on file.
No exceptions noted.

Safeguarding assets

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

Process description

On receipt of the fee, invoice or levy documentation, the pension administrator checks the details for reasonableness. Authorisation is obtained from the client before the pension administrator arranges payment from the scheme bank account. In some instances the client may provide blanket consent for regular fees, invoices or levies. The pension administrator will check that there are sufficient funds in the bank account before raising payment.

Control activity	Auditor testing
4.12 - Authorisation for payment of scheme fees, invoices or levies is obtained before arranging payment from scheme funds. A Fee / invoice / levy payment eChecklist is used to record the completion of each step of the process and the file is marked accordingly by the processor and reviewer.	**4.12** - For a sample of scheme fees, invoices or levies, obtained a copy of the corresponding eChecklist and confirmed that in all cases the eChecklist had been completed and independently reviewed. Confirmed that the eChecklist was marked accordingly by the processor and reviewer. No exceptions noted.

Safeguarding assets

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

Process description

Documentary evidence is obtained before paying retirement benefits, death benefits and transfers. Evidence requirements for each process are identified on the eChecklist completed by the pension administrator for the task in question (e.g. retirement, death, transfer out). Where required, trustee and company consent is obtained by the pension administrator prior to payment.

Additional due diligence checks are carried out on receipt of a request for a transfer value payment.

Control activity	Auditor testing
4.13.1 - Documentary evidence supporting the payment request is reviewed for validity by a second pension administrator, which is recorded on the file. Barnett Waddingham authorisers will not authorise payment requests without a documented review check.	**4.13.1** - For a sample of payment requests, evidence was reviewed to confirm each request had been subject to review by an independent second pension administrator, to confirm validity. No exceptions noted.
4.13.2 - Following a request for a transfer value payment, a series of risk-based checks are performed by the pension administration team which are recorded on the eChecklist. If appropriate, suspicious cases are escalated to the Technical Team for further investigation.	**4.13.2** - For a sample of transfer payments, evidence of the series of risk-based checks was confirmed as recorded on the eChecklist. No suspicious cases requiring escalation were identified in the sample tested. No exceptions noted.

Safeguarding assets

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

Process description

Evidence of continued entitlement checks for pensioners are performed by pension administrators to ensure recipients are still eligible for benefit payments. Methodologies may include the use of third party data cleansing services, letter mailings or third-party tracing services.

Where evidence of continued entitlement has not been received from a pensioner, the pension administrator refers to the client to agree the appropriate action which may range from further enquiries to suspension of payments.

Alternatively if a child fails to provide adequate evidence of educational status, further payments may be suspended without prior reference to the trustees.

Control activity	Auditor testing
4.14.1 - On a frequency agreed with the client the pension administrator validates the entitlement of members to continued benefit payments. Methodologies may include the use of third party data cleansing services, letter mailings or third-party tracing services.	**4.14.1** - For a sample of schemes, evidence of the administrator validating the entitlement of members to continued benefit payment was obtained and confirmed this was in line with the frequency agreed with the client. No exceptions noted.
4.14.2 - The pension administrator obtains client consent, which is retained on the file, before suspending payments.	**4.14.2** - For a sample of member benefit payment entitlement checks, evidence was obtained to confirm that client consent had been obtained prior to payments being suspended. No exceptions noted.
4.14.3 - Where a child's pension is subject to educational status, evidence of continued entitlement is sought annually by the pension administration team from the child or their parent or guardian and the educational body.	**4.14.3** - For a sample of children's pensions that were subject to educational status, confirmed evidence of continued entitlement had been sought by the administrator annually from the child, their parent/guardian or the educational body. No exceptions noted.

Safeguarding assets

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

Process description

On receipt of a pension payslip or other pensioner correspondence returned undelivered by the post office, the pension administrator assesses the individual circumstances to determine the appropriate action and timescale. Traces may be attempted via the Department for Work and Pensions, third party tracing services and the pensioner's bank. During the investigative process carried out by the pension administrator, and in timescales appropriate to the circumstances, the pension administrator will obtain instruction from the client regarding the possible suspension of payments until the pensioner can be traced.

If a Bacs pension payment is returned unpaid, or a child fails to provide adequate evidence of educational status, further payments may be suspended without prior reference to the trustees. The pension administrator will then take appropriate steps to investigate the pensioner's status, in line with the principles set out above.

Control activity

4.15 - The suspension of a payroll member is processed by a pension administrator and input to Penstream. A second pension administrator checks the validity of the suspension, and the existence of consent (where needed), before applying the change to the system. The system does not allow a single pension administrator to apply the change directly.

Auditor testing

4.15 - Through observation, confirmed suspensions were processed within Penstream by a pension administrator and were subject to validity checks and existence of consent by an independent second pension administrator, prior to the change being applied. Confirmed that validity/ reason for suspension and existence of consent (where needed) was required before a member record could be suspended. This is logically enforced within the system.
No exceptions noted.

Managing and monitoring compliance and outsourcing

Receipts of contributions are monitored against required timescales

Process description

Contributions are paid in accordance with a schedule agreed between the employer and the trustees with member contributions having to be paid to the trustees before the statutory deadline in the month following the deduction of the contributions from members' pay. A scheduled task activates and is assigned to the nominated pension administrator before contributions are due each month, or less often as determined by the schedule. Progress is monitored against deadlines by the nominated pension administrator or Team Leader.

Control activity

5.01 - A regular scheduled task is used to prompt monitoring when contributions are due and a contribution monitoring file is maintained to record contribution due dates and receipts. When contribution payment notifications are received, the pension administrator records the date on which they are received in the contribution monitoring file. Any missing contributions are pursued with the client.

Auditor testing

5.01 - For a sample of schemes, confirmed the regular scheduled task was set up. The contribution receipts monitoring file was obtained for all sites, for a sample of schemes across a sample of months, confirmed that date of when contributions were received were recorded.
No exceptions noted.

Managing and monitoring compliance and outsourcing

Receipt of contributions, in accordance with schemes rules and legislative requirements, are monitored

Process description

Contributions are paid in accordance with a schedule agreed between the employer and the trustees with member contributions having to be paid to the trustees before the statutory deadline in the month following the deduction of the contributions from members' pay.

Control activity	Auditor testing
5.02 - Late contributions are reported to the partner responsible for the client or their delegate who considers such reports in accordance with the principles of the traffic light framework put in place by TPR.	**5.02** - For a sample of late contribution, confirmed that the late contributions have been reported to the partner and followed up on. No exceptions noted.

Managing and monitoring compliance and outsourcing

Receipt of contributions, in accordance with schemes rules and legislative requirements, are monitored

Process description

Contributions received are checked by the pension administrator for reasonableness against the requirements of the schedule.

For DB schemes with active members, the pension administrator spot checks individual member contributions annually for accuracy or reasonableness by comparison with the percentage of pensionable salary defined in the scheme rules and set out in the schedule of contributions.

For DC schemes the Penstream member record includes pensionable salary and contribution percentage data, from which the system can predict expected contributions. Contribution receipts are loaded to member records on Penstream and the system generates exception reports of any contributions falling outside reasonable tolerance bands.

Control activity	Auditor testing
5.03.1 - For DB schemes, member contributions received are spot checked by the pension administration team for reasonableness during the annual renewal which takes place following a scheme's anniversary date. Member contributions are checked against the requirements of the schedule of contributions and any discrepancies are raised with the client. Contribution checks and evidence of their review are retained and the file is marked accordingly by the processor and reviewer.	**5.03.1** - For a sample of DB schemes with active members, evidence of the administrators' annual spot checks on individual member contributions was confirmed, along with evidence of independent review. Confirmed evidence had been retained on the annual renewal records and the file was marked accordingly by the processor and reviewer. No exceptions noted.
5.03.2 - DC contributions received are checked for reasonableness each contribution cycle. Exceptions generated during the monthly contribution input process are reviewed by the pension administration team and any anomalies or errors are resolved with the client. A monthly contribution cycle eChecklist is used to record the completion of each step of the process and the file is marked accordingly by the processor and reviewer.	**5.03.2** - For a sample of DC schemes, and a sample of months, evidence of pension administrator review, of the exceptions generated during the monthly contribution input process was obtained and confirmed as completed. Confirmed the monthly contribution cycle eChecklist was used to record the completion of each step of the process and the file was marked accordingly by the processor and reviewer. No exceptions noted.

Managing and monitoring compliance and outsourcing

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 the standards set out in service level agreements.

Process description

A service level schedule is included as part of an Administration Agreement with the client (where the client has so requested). Taskstream worktypes are coded by Taskstream Administrators with the agreed service levels for tasks.

The pension administrator logs all tasks and enquiries daily onto Taskstream which allocates a turnaround time specific to the scheme's agreed service level agreement. Team Leaders review current work in progress on Taskstream and are responsible for agreeing any prioritisation of ad hoc tasks with clients. Service levels are reported as part of the administration report where the client so requests (see 6.01).

Control activity	Auditor testing
5.04 - Access to create or amend Taskstream worktype coded service levels is restricted to Taskstream Administrators.	**5.04** - Through discussion with management and review of the Taskstream permission group, confirmed that only Taskstream Administrators have access to create or amend Taskstream Worktype coded service levels. No exceptions noted.

Managing and monitoring compliance and outsourcing

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

Process description

Feedback from clients and members, both positive and negative, including transaction errors is recorded on a centralised Administration Feedback database. Incidents identified internally, including transaction errors are also recorded on the Administration Feedback database as soon as they are discovered. Remedial action is agreed between the partner, Client Relationship Manager, Team Leader and pension administrator to address the incident (in consultation with the client if appropriate).

New additions to the Administration Feedback database are automatically notified by email to the partner responsible for the client, and an entry created on the Governance Team's database for consideration. Barnett Waddingham's response to formal complaints is processed in accordance with regulatory and statutory obligations under the Governance Team's supervision. Other incidents are managed locally, with monitoring by the Governance Team where appropriate.

Root cause analysis is performed by the Quality Assurance Analyst who reports statistics and observations to the PAPG.

Control activity	Auditor testing
5.05.1 - The Quality Assurance Analyst receives a copy of the email notification in order that they may consider the causes and effects of incidents, carry out risk and impact assessments as appropriate and instigate changes to procedures when determined to be necessary.	**5.05.1** - For a sample of incidents, evidence of notification to the Quality Assurance Analyst was obtained. For each incident it was confirmed the Quality Assurance Analyst had carried out a risk and impact assessment as appropriate and instigated changes to procedures where deemed necessary. No exceptions noted.
5.05.2 - The Quality Assurance Analyst produces a report containing incident statistics and feedback that they submit in advance of PAPG meetings, which occur three times a year.	**5.05.2** - Evidence of the PAPG meeting minutes for two instances were obtained to confirm the PAPG's reviews of the incident report statistics and feedback produced by the Quality Assurance Analyst. No exceptions noted.
5.05.3 - On receipt of a new incident report the Quality Assurance Analyst or Governance Team review the circumstances of the case and determine if it is to be dealt with as a formal complaint. Records of correspondence and actions taken on formal complaints are maintained. Monthly and quarterly complaint analysis reports are produced by the Governance Team for business area leaders and the PRCC. Copies of all reports and their issue are retained by the Governance Team.	**5.05.3** - For a sample of months, evidence was obtained to confirm the monthly complaints update was reviewed by the Governance Team and also submitted to the Partner nominated to oversee the complaint handling. For a sample of months and quarters, confirmed reporting had been produced and submitted to the PRCC. No exceptions noted.

Managing and monitoring compliance and outsourcing

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

Process description

When the partner or Team Leader responsible for the client considers appropriate remedial action following an incident, they have due regard for the impact (if any) on the client. The consequences of the incident are reviewed and a report is made to the client when considered appropriate. Compensatory terms may be agreed with the client if considered necessary, subject to any regulatory or legal issues which may be raised by the Governance Team.

Control activity	Auditor testing
5.06 - A partner, principal or associate reviews the circumstances resulting in an error, determines an appropriate level of compensation and agrees this with the client if circumstances warrant it. Settlement of compensation is arranged by, or under the supervision of, the partner e.g. by adjustment to fee invoices, payment from Barnett Waddingham company account.	**5.06** - For a sample of compensation payments, confirmed that partner approval had been sought and obtained prior to the settling of compensation payments. No exceptions noted.

Managing and monitoring compliance and outsourcing

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

Process description

The core procedural guides (e.g. Whistleblowing, Anti-Money Laundering, Complaints, Conflicts, Personal Investment Shares and Market Abuse) are held in the Policy Handbook on Barnett Waddingham’s intranet. The Whistleblowing manual includes guidance regarding possible reportable breaches and pension administrators’ obligations regarding the reporting thereof.

All new employees are referred to these procedural guides and receive training as part of their induction.

Control activity

5.07 - The procedural guides are updated when required as a result of changes in Barnett Waddingham’s policy or regulatory compliance requirements, and reviewed at least annually by the Compliance Officer for continued validity. Completion of the review is reported to the other members of PRCC by the Compliance Officer as part of the quarterly report which is reviewed at a PRCC meeting and minuted accordingly.

Auditor testing

5.07 - For a sample of quarters, obtained the PRCC quarterly report and corresponding meeting minutes. Confirmed the procedural guides had been subject to at least an annual review by the Compliance Officer.
No exceptions noted.

Managing and monitoring compliance and outsourcing

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

Process description

The partner responsible for the client, their delegate or the Scheme Actuary maintains an electronic file of all breach reports received. Reports are retained on file after they have been considered for possible reporting.

Control activity	Auditor testing
5.08 - Breach reports are reviewed by the partner responsible for the client, their delegate or the Scheme Actuary. Decisions taken as to whether a report of the incident should be made, in accordance with the principles of the traffic light framework put in place by TPR, are recorded. Copies of reports are retained by the partner, or their delegate, to facilitate further review if an accumulation of incidents becomes evident.	**5.08** - For a sample of breaches, confirmed that a breach report had been prepared and reviewed by an appropriate individual. Confirmed that review was performed timely and the decision was documented and made in accordance of traffic light framework No exceptions noted.

Managing and monitoring compliance and outsourcing

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

Process description

Code of Practice 02 issued by TPR outlines a number of designated notifiable events which must be reported. The eChecklists covering processes which are potentially subject to regulatory reporting include reminders to the pension administrator to consider reporting requirements during processing. When the pension administrator processes a transaction potentially subject to notification requirements, they liaise with the partner or Client Account Manager responsible for the client. The partner, Client Account Manager or their actuarial assistant, reviews the circumstances of the transaction in conjunction with the pension administrator in order to determine whether it constitutes a notifiable event and arrange for a notification to be submitted to TPR on behalf of the client where appropriate.

Control activity

5.09 - Notifiable event reporting forms, where prepared in the Pension Administration Business Area, are reviewed by an experienced pension administrator and/or the partner prior to submission to TPR. A TPR notifiable event eChecklist is used to record the completion of each step of the process and the file is marked accordingly by the processor and reviewer.

Auditor testing

5.09 - For a sample of notifiable events, evidence was obtained to verify that a notifiable event reporting form had been prepared and reviewed. Confirmed a TPR notifiable event eChecklist was used to record the completion of each step of the process and the file was marked accordingly by the processor and reviewer.
No exceptions noted.

Reporting to clients

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

Process description

Administration reporting requirements are agreed between the client, the partner responsible for the client, and where appropriate the Team Leader.

Administration reports are prepared by the pension administrator at a frequency agreed with the client and include information regarding service level performance, as required by the client.

Control activity	Auditor testing
6.01 - Administration reports are reviewed for completeness and accuracy prior to being issued to the client and the review is marked on file by the reviewer.	**6.01** - For a sample of administration reports, confirmed that they were independently reviewed prior to issue to the client and that file had been marked by the reviewer. No exceptions noted.

Reporting to clients

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

Process description

Annual benefit statements, where required by statutory regulations or by the client, are prepared by the pension administrator in accordance with the requirements of the client and issued in line with applicable statutory requirements. Progress and completion of the task on Taskstream is monitored against agreed service levels and statutory timescale requirements under the supervision of Team Leaders.

Statement formats are customised to the client's requirements, but some components for DC schemes are imported from generic system standard documentation. Any modification to the generic system documentation is agreed with, and implemented by, the Document Automation Support team.

Control activity	Auditor testing
6.02.1 - The preparation of benefit statements, including spot checks of Penstream calculations for reasonableness or accuracy, is reviewed by the pension administration team prior to production. If requested, the client also reviews the benefit statement format and content prior to issue. The file is marked accordingly by the processor and reviewer.	**6.02.1** - For a sample of schemes, confirmed that benefit statement had been subject to independent review prior to production and the file had been marked accordingly by the processor and reviewer. No exceptions noted.
6.02.2 - The pension administrator submits a request to the Document Automation Support team for modification to a standard document where required. The Document Automation Support team implement the change. A BWWord Support Request eChecklist is used to record the completion of each step of the process by the processor and reviewer.	**6.02.2** - For a sample of changes made to standard documentation, inspected the BWWord Support Request eChecklist and confirmed this was used to record the completion of each step of the process by the processor and reviewer. No exceptions noted.

Reporting to clients

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

Process description

Annual reports and accounts are prepared for all clients using a standard template, compliant with the requirements of the SORP, or as otherwise agreed with the client and their appointed auditor. A separate template is maintained for PPF clients.

The templates are reviewed against changes in the SORP when they occur and feedback received from auditors on an ongoing basis. Most pension administrators have read-only access to the templates. Permission to edit the templates is restricted to authorised users by system permission settings (see 7.12).

Control activity	Auditor testing
6.03 - Modifications to the report and accounts templates are carried out by pension administrators with specialist knowledge of pension scheme accounting techniques and checked for accuracy by a member of the Pension Accounts Group Technical Committee.	**6.03** - Modifications to the standard generic template were obtained. It was confirmed that the modifications were authorised and checked for accuracy by a member of the Pension Accounts Group Technical Committee. No exceptions noted.

Reporting to clients

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

Process description

At the end of each scheme year, as required, a timetable for completion and audit of the accounts is agreed between a member of the Pension Accounts Group and the auditor. Progress of work on the report and accounts is monitored on Taskstream against agreed service levels and statutory timescale requirements, under the supervision of the Team Leader. The report and accounts are prepared by a member of the Pension Accounts Group and completed and signed off by the client’s appointed auditor within the statutory seven month limit.

Control activity	Auditor testing
6.04.1 - The draft report and accounts are reviewed for completeness against the requirements of the SORP accounting standards and for accuracy of numerical contents by the pension administration team. The file is marked accordingly by the processor and reviewer prior to submission to the client's appointed auditor.	**6.04.1** - For a sample of schemes, inspected the eChecklist and confirmed that the accounts had been independently reviewed prior to the submission to the client's external auditor. No exceptions noted.
6.04.2 - Breaches of the statutory seven month deadline are reported to the partner responsible for the client, or their delegate. The partner, or their delegate, considers whether the breach should be drawn to the client’s immediate attention in line with TPR’s whistleblowing guidance.	**6.04.2** - For a sample of breaches to the statutory seven month deadline, confirmed that the breaches had been reported to the Partner, and marked as approved in the breach log. No exceptions noted.

Information technology (Restricting access to systems and data)

Physical access to In-scope systems is restricted to authorised individuals

Process description

Barnett Waddingham offices are accessible using an electronic card and/or a key. While cards are issued to anyone coming into our premises, keys are allocated to staff that require them. Access levels vary depending on the type of user, their function and geographical location.

Electronic cards and keys are retrieved from staff who leave the firm and cards are deactivated.

Control activity	Auditor testing
7.01.1 - The IT department are notified of new employees by the HR department. Cards for new employees are created following the new starter process and completion of this step is recorded on an eChecklist which is subject to review.	**7.01.1** - For a sample of new starters it was confirmed that new cards issued followed the standard joiner's process with the step included on the eChecklist. No exceptions noted.
7.01.2 - A log of key holders is maintained by offices where keys are used.	**7.01.2** - The audit log, for those offices where keys are used, was obtained to confirm existence for a sample. Further inspection identified that the log is being maintained on a timely basis. No exceptions noted.
7.01.3 - The IT department are notified of staff who leave the firm by the HR department. Cards are deactivated and retrieved following the leaver process and completion of this step is recorded on an eChecklist.	**7.01.3** - For a sample of leavers it was confirmed that cards/keys are retrieved on a timely basis and in line with the leaver's process with the step included on the eChecklist. No exceptions noted.

Information technology (Restricting access to systems and data)

Physical access to In-scope systems is restricted to authorised individuals

Process description

All visitors must register their presence with local reception who allocate a temporary electronic card, granting access to specific zones if appropriate. Staff, visitors and contractors are required to wear a visible pass for the duration of their presence on site.

Control activity	Auditor testing
7.02.1 - The electronic visitor log is administered by the Secretarial Team in each office.	**7.02.1** - The visitors log was obtained and reviewed confirming ongoing update and review by each local facilities team. No exceptions noted.
7.02.2 - Activation of cards granting contractors access to specific zones is requested via the IT ticket system and approved by IT.	**7.02.2** - Walk-though testing was conducted confirming that the process for the activation of contractor and temporary staff passes is requested by facilities and approved by IT. The IT ticket system was reviewed to verify control operation. No exceptions noted.

Information technology (Restricting access to systems and data)

Physical access to In-scope systems is restricted to authorised individuals

Process description

Network devices are located in secure rooms. Access to secure rooms is restricted to IT and certain other authorised staff such as Network Administrators who have permanent access to the IT secure rooms in their designated offices.

Control activity	Auditor testing
7.03.1 - Access to secure rooms is restricted to IT staff and others in line with business needs.	**7.03.1** - Network administrator access was verified by observation of the access lists. No exceptions noted.
7.03.2 - All other access to secure rooms requires authorisation which is obtained and recorded via the IT ticket system.	**7.03.2** - Sample testing confirmed that non-network administrator access needs to be formally requested and authorised via the IT ticket system. No exceptions noted.

Information technology (Restricting access to systems and data)

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

Process description

Network access is provided through Ethernet cable or a wireless access service and is restricted to authorised personnel.

Control activity	Auditor testing
7.04.1 - Logons are unique and passwords are restricted by minimum complexity requirements. Access rights depend on the type of work individuals are required to perform.	**7.04.1** - Active Directory logical access configurations were reviewed and password complexity requirements were confirmed at the domain level, confirming logins are unique and restricted. No exceptions noted.
7.04.2 - All computers require an additional encryption pass code to be entered before a user may log on to the device.	**7.04.2** - Through observation of a sample of computers, it was confirmed encryption configurations were applied to each computer. No exceptions noted.
7.04.3 - Access to the network via the wireless access service is restricted to devices carrying the required digital security certificate. Temporary guest wireless internet access can be granted for uncertified devices but this does not provide access to the network.	**7.04.3** - Network wireless access digital security certificate configurations were reviewed, confirming access to the network via the wireless access service is restricted. No exceptions noted.

Information technology (Restricting access to systems and data)

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

Process description

Access to all networked software needs signing onto the network with logon and password.

Control activity	Auditor testing
7.05.1 - New accounts are created by following the new starter process and actions recorded on an eChecklist which is subject to review.	**7.05.1** - For a sample of new accounts, it was confirmed they were created by following the formal joiner's process with actions recorded on an eChecklist. No exceptions noted.
7.05.2 - Periodic integrity checks are performed on user accounts and any actions taken on exceptions are documented.	**7.05.2** - Integrity (consistency) checks were confirmed to be performed on user accounts with a supporting exception escalation process. No exceptions noted.

Information technology (Restricting access to systems and data)

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

Process description

Some applications require additional user privileges and password security. Browser based software provided by third party suppliers utilises extra security measures, to prevent unauthorised access.

Control activity	Auditor testing
7.06.1 - The Bacs processing system has additional password, user privilege and access controls which are allocated and maintained by Bacs System Administrators, and further access restriction using Bacs smartcard technology.	**7.06.1** - Observed the Bacs processing system confirming additional password, user privilege and access controls are in place. No exceptions noted.
7.06.2 - STP has additional password, user privilege and access controls which are allocated and maintained by STP System Administrators, and further access restriction using IP and certificate controls which are maintained by Network Administrators.	**7.06.2** - The STP procedure log was reviewed to confirm access controls. STP requires a security certificate to be installed and also an authorised IP address. No exceptions noted.
7.06.3 - The CCM Browser has additional password, user privilege and access controls which are maintained by authorised users and Gatekeepers.	**7.06.3** - Controls evaluation and testing identified that the CCM browser is used for payments from the client’s pooled banking account. The CCM account is only accessible internally to the client's network. Access is enforced through permissions within the system. A username and password is required to access the web application. No exceptions noted.

Information technology (Restricting access to systems and data)

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

Process description

All staff are issued laptop computers that have encryption protection to prevent unauthorised access to data in the event of loss or theft. Measures are in place to protect unattended computers.

Members of staff are required to familiarise themselves with Barnett Waddingham's Laptop Policy and acknowledge that they have done so.

Control activity	Auditor testing
7.07.1 - Password protected screen savers run on all servers, desktop PCs and laptop computers after a defined period of inactivity.	**7.07.1** - Observed that configuration settings exist for all end-users that includes password protected screensaver configurations. No exceptions noted.
7.07.2 - A log of users' policy acknowledgements is retained and scheduled weekly tickets are used by either the IT Support team or HR team to identify and resolve overdue policy acknowledgements.	**7.07.2** - For a sample of staff, it was confirmed that policy acknowledgements were retained and documented. No exceptions noted.

Information technology (Restricting access to systems and data)

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

Process description

Some components of Penstream can be accessed via the internet by clients (e.g. trustees and human resources personnel) and, with client approval, by members. New account creation is handled following a standard procedure. Accounts are unique to each person.

Outgoing member data transmitted by digital or electronic means is encrypted (see 7.16).

Control activity	Auditor testing
7.08.1 - Accounts are accessed via a two-step login process and lock outs are in place after successive failed login attempts.	**7.08.1** - Controls verification confirmed that two factor password restrictions and failed log-in controls are in place and operational. No exceptions noted.
7.08.2 - Standard procedure is followed to grant members access to their records.	**7.08.2** - Confirmed that an Invitation is required from within Penstream as a result of instructions from client. This generates a letter and sends the information to create an account by the client with the details from Penstream. No exceptions noted.
7.08.3 - The BWebstream registration portal is subject to an annual penetration test. Test results are reviewed and actions identified where required and logged. The reports are also reviewed by the IT Committee and noted in meeting minutes.	**7.08.3** - The latest penetration test was obtained and action planning was confirmed to be in place. Testing confirmed that penetration testing results were included in the IT Committee agenda with supporting follow up action planning. No exceptions noted.

Information technology (Restricting access to systems and data)

Segregation of incompatible duties within and across business and technology functions is formally defined, implemented, updated and enforced by logical security controls

Process description

Penstream is an information system, database, calculator and report/letter production tool only. Other administrative duties (e.g. payments) are handled outside the system (see 4.11 and 7.11) by authorised staff and in accordance with the processes and controls for those duties. Within the Penstream application, high risk modifications have inbuilt logical controls to segregate duties.

Control activity

7.09 - Modifications to bank account details, additions of new members to payrolls and suspension/unsuspension of payments are processed by the administrator and input to the system. The inputs are reviewed for accuracy by another administrator who then applies the change to the system.

Auditor testing

7.09 - Through discussion with management the separation of duties process was confirmed. By inspection of the Penstream security module verified the restrictive setting that enforces changes to bank account details have to be made by at least two accounts.
No exceptions noted.

Information technology (Restricting access to systems and data)

Segregation of incompatible duties within and across business and technology functions is formally defined, implemented, updated and enforced by logical security controls

Process description

User access within Penstream is restricted based on experience and business needs. Functionality restrictions are used to enhance security, reduce errors, and provide protection of personal data.

Control activity	Auditor testing
7.10 - Permissions for different users are authorised, allocated and maintained by group managers in UaG.	**7.10** - Through system configuration observation for the Penstream Security user account management, the separation of duties process was confirmed by assessment of related user profiles and observation. The Penstream security module was observed and inspection confirmed that only Penstream Security Users can access and amend user access permission. No exceptions noted.

Information technology (Restricting access to systems and data)

Segregation of incompatible duties within and across business and technology functions is formally defined, implemented, updated and enforced by logical security controls

Process description

Barnett Waddingham is an authorised Bacs Bureau. Access to the Bacs processing system software is limited to authorised staff and is protected by a combination of independent security layers (see 7.06.1).

Control activity	Auditor testing
7.11.1 - Access to the Bacs processing system software is controlled by the IT department. Any changes are recorded in the IT ticket system.	**7.11.1** - A controls evaluation assessment confirmed that access to the restricted server from which the Bacs system software operates is controlled. Testing confirmed that changes are recorded in the IT ticket system. No exceptions noted.
7.11.2 - Creators and Senders require an access smartcard and accompanying PIN. Bacs smartcard allocation is controlled. Each card user can either create or authorise Bacs submissions, not both.	**7.11.2** - Through system configuration observation, the separation of duties process was confirmed by assessment of related user profiles and observation. Sample testing was also undertaken for smart card authorisation. No exceptions noted.

Information technology (Restricting access to systems and data)

Segregation of incompatible duties within and across business and technology functions is formally defined, implemented, updated and enforced by logical security controls

Process description

Standard report and accounts templates, compliant with the requirements of the SORP, are maintained for use on all clients. Most pension administrators have read-only access to the templates. Permission to edit the templates is restricted to authorised users by system permission settings.

Control activity	Auditor testing
7.12 - The ability to add or remove users from the editing group is restricted by system permission settings to authorised users.	**7.12** - Review of the system configuration confirmed access add or remove users from the editing group is restricted. No exceptions noted.

Information technology (Maintaining integrity of the systems)

Scheduling and internal processing of data is complete, accurate and within agreed timescales

Process description

PAYE taxation submissions are transmitted electronically to HMRC Online Services following GovTalk data transmission protocols. The HMRC Online Services Transaction Engine returns the completion status for each report which is recorded by the BW GovTalk Submitter.

Control activity	Auditor testing
7.13.1 - The ability to release submission files is restricted to authorised staff. Access restrictions are logically enforced by the system and maintained by group managers in UaG.	**7.13.1** - Through system configuration observation, system access is limited to a small number of people. Through enquiry of management it was confirmed that the individuals assigned with this permission are appropriate. No exceptions noted.
7.13.2 - The Payroll Administrator checks submission files daily and authorises their release to HMRC Online Services. The Payroll Administrator monitors the completion status of all submissions and reports any failures to the relevant team.	**7.13.2** - Through system configuration observation, system access configurations were evaluated and monitoring controls were verified. By observation, the submission file checking and monitoring process was verified. It was confirmed that issues are automatically logged with the IT ticket system. No exceptions noted.
7.13.3 - In the event of a communication failure between the BW GovTalk Submitter and HMRC Online Services an error report is generated and submitted to the IT ticket system. An investigation and resolution of any such reported failure is carried out and recorded in the IT ticket system.	**7.13.3** - A ticket from the IT ticket system was inspected to confirm that any submission failures are followed through to resolution. No exceptions noted.

Information technology (Maintaining integrity of the systems)

Scheduling and internal processing of data is complete, accurate and within agreed timescales

Process description

HMRC's Data Provisioning Service (DPS) is used for the receipt of electronic PAYE notifications.

Control activity	Auditor testing
7.14.1 - In the event of a communication failure with the DPS system an automated error report is generated by the system and submitted to the IT ticket system for resolution.	**7.14.1** - The automated error notification process was inspected (emails are sent notifying of success/failure). We confirmed that issues are logged within the IT ticket system. No exceptions noted.
7.14.2 - Notices that could not be processed automatically are reported for manual adjustment as required. As part of the regular payroll process, at a frequency agreed with the client, the administrator checks for unprocessed notices and records the check on the Payroll run eChecklist.	**7.14.2** - An outlook folder holds records of processing. The emails headers were reviewed and evidence of completed downloads for the period sampled was noted. Details of the updates were confirmed to have been provided in the email. It was also confirmed that payroll eChecklists included a review of unprocessed notices. No exceptions noted.

Information technology (Maintaining integrity of the systems)

Scheduling and internal processing of data is complete, accurate and within agreed timescales

Process description

Automated background server processes are monitored for continued operability.

Control activity	Auditor testing
7.15 - The server processes managing communications with the DPS and HMRC Online Services are continuously checked by network monitoring software. Errors are reported automatically for remediation action to take place.	**7.15** - Through system configuration and process observation it was confirmed that the gateway is monitored and that checking processes exist. No exceptions noted.

Information technology (Maintaining integrity of the systems)

Transmission of data to/from external parties is complete, accurate, executed within agreed timescales and secure in line with external party agreements

Process description

Outgoing member data transmitted by digital or electronic means is encrypted or password protected. Files may be transferred via email (see 4.04.1), BWebstream or API services.

Online functionality within Member self-service is used to exchange member data and correspondence with members who have online access and SFX is used for clients and authorised third parties.

Some letters generated by Penstream are sent using a third party mailing service utilising an API.

Control activity	Auditor testing
7.16.1 - All transmissions of data through the online services available via the BWebstream registration portal are sent using HTTPS secure channels.	**7.16.1** - System observation confirmed secure transfer controls are in place. On logging in it was noted that HTTPS was utilised. The certificate for the BWebstream registration portal was also viewed and verified. No exceptions noted.
7.16.2 - All transmissions of data to the third party print and mailing service are sent using HTTPS secure channels.	**7.16.2** - Observed the mailing service transmission code confirming HTTPS channels in use. No exceptions noted.

Information technology (Maintaining integrity of the systems)

Transmission of data to/from external parties is complete, accurate, executed within agreed timescales and secure in line with external party agreements

Process description

Data in respect of PAYE taxation is transmitted to HMRC Online Services. Following submission, the completion status of each report is confirmed by HMRC Online Services (see 7.13).

Control activity	Auditor testing
7.17 - Electronic data transmissions are made over the internet using HTTPS secure channels.	**7.17** - System observation confirmed HTTPS secure channels are in place. No exceptions noted.

Information technology (Maintaining integrity of the systems)

Transmission of data to/from external parties is complete, accurate, executed within agreed timescales and secure in line with external party agreements

Process description

HMRC tax code notifications are retrieved on a daily basis using a scheduled service. Error reports are generated by the system (see 7.14.1).

Control activity	Auditor testing
7.18.1 - Electronic data transmissions are made over the internet using HTTPS secure channels.	**7.18.1** - System observation confirmed HTTPS secure channels are in place. No exceptions noted.
7.18.2 - HMRC's DPS system supplies unique incremental data block IDs, the highest of which is noted in each retrieval exercise and used as the starting point for the next retrieval exercise to ensure all new records are present.	**7.18.2** - System observation confirmed ID controls. A web service call is made to the DPS system. The XML response is saved as an audit trail. This file is named DPS_Status.xml. There is a sequential number in the relevant XML entities for all the schemes and also for the yearly P9 data. These high water marks are designed to allow the application to process new or missing data only. No exceptions noted.

Information technology (Maintaining integrity of the systems)

Data received from external parties is scanned for known vulnerabilities, any compromised data is quarantined and definitions of threats are periodically updated

Process description

All incoming data is checked for known viruses prior to transmission or release to the network.

Control activity	Auditor testing
7.19.1 - Incoming emails are scanned by the service provider to identify potential threats. Files opened via email are subject to on-access scanning to identify potential threats.	**7.19.1** - Email controls were confirmed by system observation and walk-though testing. No exceptions noted.
7.19.2 - Emails containing known viruses are logged, blocked and deleted by the email service provider.	**7.19.2** - Email controls for known virus incidents were confirmed by system observation. No exceptions noted.
7.19.3 - Files received through Member self-service and SFX via the BWebstream registration portal are virus scanned during the transmission process to identify potential threats.	**7.19.3** - Observed the configuration for files received through the BWebstream registration portal confirming they are virus scanned during the transmission process to identify potential threats. No exceptions noted.

Information technology (Maintaining integrity of the systems)

Data received from external parties is scanned for known vulnerabilities, any compromised data is quarantined and definitions of threats are periodically updated

Process description

New client data received on hard storage media is scanned for viruses. The majority of removable media devices are disabled using device control software. Staff with a legitimate business need are granted controlled access rights to such peripheral devices.

Control activity	Auditor testing
7.20 - Access privileges require authorisation through the IT ticket system by a partner, principal or associate on the IT Committee or IT Team Leader and are created on a temporary basis.	**7.20** - For a sample of removable media access requests, it was confirmed appropriate approval was sought. No exceptions noted.

Information technology (Maintaining integrity of the systems)

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

Process description

Cloud-based virus protection is automatically kept up to date with cloud native architecture and using a SaaS delivery model.

Control activity	Auditor testing
7.21 - Email alerts are triggered in the event a virus is found. Notifications are sent to our Security Operations Centre (SOC) service for review and necessary action is taken. Machines are isolated from the network if necessary.	**7.21** - Observed the configuration and a sample confirming email alerts are triggered in the event a virus is found. The notifications settings include emailing the Security Operations Centre (SOC) service for review. No exceptions noted.

Information technology (Maintaining integrity of the systems)

Network perimeter security devices are installed and changes are tested and approved

Process description

Network penetration testing is commissioned twice a year and carried out by external network security experts. Multiple service providers are used in order to obtain expanded test coverage.

Control activity

7.22 - The network penetration testing reports are reviewed to identify any actions required. High and medium risk items always require action and will be logged on Taskstream. The reports are reviewed by the IT Committee and any where actions are required are noted in meeting minutes.

Auditor testing

7.22 - The latest penetration test was obtained and action planning was confirmed to be in place. Testing confirmed that penetration testing results were including in the IT Committee agenda with supporting follow up action planning.
No exceptions noted.

Information technology (Maintaining integrity of the systems)

Network perimeter security devices are installed and changes are tested and approved

Process description

Network hosted services are firewalled from external access.

Web filtering is used for internet access control.

Control activity	Auditor testing
7.23.1 - Changes to firewall configuration settings are recorded and authorised by a partner, principal or associate on the IT Committee.	**7.23.1** - System and process observation confirmed firewall change controls. Sample testing confirmed that changes are raised as a Request For Change (RFC), in line with the formal change management process. These are archived into Taskstream and authorised by the IT Committee. No exceptions noted.
7.23.2 - Changes to web access can be made only by Network Administrators and require authorisation by a partner, principal or associate on the IT Committee or IT Team Leader.	**7.23.2** - System observation and sample testing confirmed change to web access controls are in place. No exceptions noted.

Information technology (Maintaining integrity of the systems)

Network perimeter security devices are installed and changes are tested and approved

Process description

Barnett Waddingham internet access application is independently security tested.

Control activity	Auditor testing
7.24 - Internet access application security reports are reviewed and any identified shortcomings are rectified. Records evidencing action taken are retained.	**7.24** - Security testing was confirmed to have been undertaken in the audit year. The retest results shows that remediation actions were taken accordingly. No exceptions noted.

Information technology (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

Process description

There is a structured development cycle for Penstream. Ad hoc development requests and error reports from users are submitted via a branch of the ticket system specifically reserved for Penstream development or via the Penstream Product Owner.

A release schedule identifies development features included in each Penstream release and those planned for future releases.

All changes to Penstream source code can be traced back to the developer responsible.

Control activity	Auditor testing
7.25.1 - All development work is authorised by the project manager, IT partner, Project Planning Lead, Development Team Leader, or Head of Software Development. Work requirements, release schedules and authorisations are documented.	**7.25.1** - For a sample of changes selected it was confirmed that there was a change request documented (i.e. in IT ticket system) and, this has been approved. No exceptions noted.
7.25.2 - Changes to Penstream are developed and tested independently of the live system. The development environment is contained on a separate network.	**7.25.2** - Observation of the system confirmed that a development and test environment is in place. No exceptions noted.
7.25.3 - A standard release procedure is followed for new code to go live. The Business Signoff is recorded in an eChecklist.	**7.25.3** - For the sample of changes it was confirmed that a business sign off was recorded in an eChecklist where applicable. No exceptions noted.
7.25.4 - All changes to Penstream source code are recorded through a TFS Git pull request. All activity is recorded in TFS and enforces code review by a second developer prior to addition to the development branch.	**7.25.4** - System observation confirmed changes to Penstream source code are recorded through a TFS Git pull request. All activity is recorded in TFS and enforces code review by a second developer prior to ability to promote code into production. No exceptions noted.

Information technology (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

Process description

IT development requests and error reports relating to in-house software other than Penstream are submitted by users and recorded using the IT ticket system. Progress on software development, including other work instigated by the software development team, is recorded.

Network infrastructure maintenance and development is carried out by Network Administrators. Proactive changes, and responses to requested changes through the IT ticket system, are recorded.

Control activity	Auditor testing
7.26.1 - Non-Penstream development requirements and individual database changes are allocated to a developer by IT Team Leaders. New software and upgrades to existing software are tested prior to release into the live system, which requires the authorisation of a partner, principal or associate on the IT Committee. Testing and approval records are maintained.	**7.26.1** - Development work and release authorisation controls were verified by process observation and testing of the IT ticket system. No exceptions noted.
7.26.2 - Changes to network infrastructure require authorisation by a partner, principal or associate on the IT Committee. Affected services are identified and recorded together with details of any testing checks and authorisation.	**7.26.2** - Change controls were verified by process observation and testing via the IT ticket system linked to an IT Committee member approval. No exceptions noted.

Information technology (Maintaining and developing systems hardware and software)

Data migration or modification is authorised, tested and, once performed, reconciled back to the source data

Process description

System maintenance or development activities requiring migration or modification of client data are rare. An audit trail is maintained for any such activities, which are authorised and checked by staff appropriate to the nature of the change.

Control activity

7.27 - System maintenance or development activities requiring migration or modification of client data are performed by either IT or specialist Pension Administration staff. Details of the change, together with authorisation and any testing or verification activities are recorded on either the IT ticket system or Taskstream.

Auditor testing

7.27 - Management confirmed that no data migration activities were performed during the audit period, therefore this control was not tested. Management confirmed that the control would still operate as described.

Information technology (Maintaining and developing systems hardware and software)

Changes to existing In-scope systems, including hardware upgrades, software patches and direct configuration changes, are authorised, tested and approved in line with policy

Process description

IT system changes relating to infrastructure are submitted by Network Administrators using the IT ticket system or Request for changes process. Changes are recorded.

Control activity	Auditor testing
7.28 - Changes to systems require authorisation by a partner, principal or associate on the IT Committee. Affected services are identified and recorded together with details of any testing checks and authorisation.	**7.28** - Change controls were verified by process observation and testing via the IT ticket system linked to an IT Committee member approval. No exceptions noted.

Information technology (Recovering from processing interruptions)

The physical IT equipment is maintained in a controlled environment

Process description

Network devices including servers, routers and switches are located in secure rooms which include processes designed to support the Confidentiality, Integrity and Availability of data services. Access to secure rooms is restricted (see 7.03).

Control activity	Auditor testing
7.29.1 - Fire extinguishers are routinely inspected and maintained in accordance with manufacturers instructions and fire safety regulations. Maintenance by a competent person is performed at least annually and a record of this work is retained.	**7.29.1** - Evidence was obtained to confirm fire extinguishers serviced in accordance with the timing requirements for our period of review. No exceptions noted.
7.29.2 - UPS devices are linked to the network to report device status and power events. Network Administrators are alerted to critical UPS functionality incidents by the automated email system and/or by audible/visual alarm reports from local staff.	**7.29.2** - UPS controls were confirmed by system observation. Alerting configurations were verified (responsibility of network administrators) and automated email configurations were verified by observation. No exceptions noted.
7.29.3 - Temperature and moisture readings outside specified thresholds as well as any detected water ingress are monitored by Network Administrators.	**7.29.3** - System observation confirmed temperature and moisture controls are in place. No exceptions noted.
7.29.4 - At periodic intervals a Network Administrator checks each secure room for unexpected audio activity. The IT ticket system is used to schedule and record completion of the checks.	**7.29.4** - Observation and testing of the IT ticket system confirmed that unusual audio activity monitoring is in place. No exceptions noted.

Information technology (Recovering from processing interruptions)

In-scope systems and data are backed up and tested such that they can be restored completely and within agreed timescales

Process description

Backup servers are managed by a third party supplier. The servers are configured to back up a selection of data from the firm's server estate. Incremental backups run daily to collect copies of new and updated data, which is held on third party backup servers, the contents of which are copied and uploaded to a co-managed cloud storage facility.

Control activity	Auditor testing
7.30.1 - Backup service reports are reviewed daily and results are kept on record.	**7.30.1** - Sample testing confirmed that backup service reports are received on a daily basis and reviewed. No exceptions noted.
7.30.2 - Integrity of the third party server backups is checked at least monthly by performing a restoration of sample data. The results are documented and any failures are investigated.	**7.30.2** - Sample testing confirmed that restore testing is carried out on a monthly basis. No exceptions noted.
7.30.3 - Backups are retained on third party servers for at least thirty days.	**7.30.3** - Inspection of the backup configuration confirmed that data back-ups are maintained for 30 days. No exceptions noted.
7.30.4 - Each year a full backup snapshot is taken and stored by the service provider, segregated from all other existing backups.	**7.30.4** - Annual full back-ups were confirmed by review of the backup solution. No exceptions noted.

Information technology (Recovering from processing interruptions)

Performance and capacity of In-scope systems are monitored and issues are resolved

Process description

Networked hardware is monitored for connectivity. Monitoring tools operate on servers with performance indicators and exceptions being reported.

Control activity	Auditor testing
7.31.1 - Networked hardware devices are interrogated on an ongoing basis for continued connectivity, performance, and capacity. The data is monitored and where issues are identified they are remediated by Network Administrators.	**7.31.1** - The system for reviewing connectivity and capacity was verified by observation of the system and resulting system output evidence. No exceptions noted.
7.31.2 - Email efficiency is measured by queue length. An automated alert is sent if the queue length exceeds our maximum tolerance and a Network Administrator investigates the cause of delays or transmission failures and resolves or escalates as required.	**7.31.2** - The maximum tolerance controls were verified by inspection of the application configuration management system. Automatic notifications were confirmed. No exceptions noted.

Information technology (Recovering from processing interruptions)

IT related Disaster Recovery Plans are documented, updated, approved and tested

Process description

The servers and services are provided through the data centre located within purpose-built facilities. A third party data centre is used for recovery. In the event of the failure of a physical server, functionality is temporarily transferred to the alternative data centre or other physical servers. IT infrastructure and data centres facilitate the continuation of business operations from another location in the event of a disaster at any individual office. The IT Operations team maintains disaster recovery procedure documentation covering the different IT systems and their recovery processes.

Control activity

7.32 - A disaster recovery simulation is carried out at least annually by Network Administrators. Outcomes for each disaster recovery simulation are documented and the results are reviewed by the IT Committee. Issues arising from a simulation are addressed. The IT disaster recovery documentation is maintained by Network Administrators under the supervision of the IT partner.

Auditor testing

7.32 - The disaster recovery test simulation was verified by review of the simulation report and evidence of IT Committee review obtained.
No exceptions noted.

Information technology (Recovering from processing interruptions)

IT related Disaster Recovery Plans are documented, updated, approved and tested

Process description

The PRCC is responsible for ensuring that a firm-wide business continuity plan is in place and that it is periodically reviewed and tested to verify its continued suitability for Barnett Waddingham's needs. The business continuity document is owned by the Information Security Manager who is responsible for maintaining and updating the plan and for organising all relevant testing.

Control activity	Auditor testing
7.33 - The business continuity plan is reviewed and tested at least annually. The Information Security Manager reports the results of all tests to the PRCC and will track and report on any recommendations or actions resulting from the tests.	**7.33** - Documentation observation confirmed that the business continuity plan has been approved by the PRCC and test results reviewed. No exceptions noted.

Information technology (Recovering from processing interruptions)

Problems and incidents relating to In-scope systems are identified and resolved within agreed timescales

Process description

All IT hardware and software issues are reported through a dedicated telephone helpdesk or via the IT ticket system.

Control activity	Auditor testing
7.34 - The IT ticket system is monitored by Network Administrators under the supervision of IT Team Leaders who are responsible for distributing and prioritising IT tasks in line with business needs.	**7.34** - For a sample of months, IT ticket system monitoring was confirmed by review of monthly reports. No exceptions noted.

Information technology (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

Process description

Some IT services and activities are outsourced to third parties who are recognised as Critical Suppliers by the new supplier process. Contracts with Critical Suppliers are agreed only once the supplier is able to fully meet Barnett Waddingham's requirements from a legal, regulatory, environmental, sustainability and Cyber Security perspective. All Critical Supplier contracts are approved by Governance and the relationship is overseen by a partner.

Management meetings are held with the service providers to review overall service provision.

Control activity	Auditor testing
7.35.1 - Critical Supplier contracts are approved by the Governance Team and the relationship is overseen by a partner. Only a partner is able to sign the contract on behalf of Barnett Waddingham.	**7.35.1** - For a sample of a new critical suppliers, it was confirmed through review of the service desk ticket that Governance reviewed and approved by the Governance Team and the contract is overseen and was signed off by a partner. No exceptions noted.
7.35.2 - Critical Suppliers engaged to provide IT services and/or products (e.g. software, hardware, hosted systems or applications) are approved by IT prior to an agreement being signed.	**7.35.2** - For a sample of a new critical suppliers, it was confirmed the contract is overseen and was signed off by a partner and included IT approval. No exceptions noted.
7.35.3 - A partner will perform or oversee a review of each Critical Supplier at least annually. Action points arising from the meetings with suppliers who provide IT services and / or products are agreed with the Head of IT Operations and any high impact or potentially disruptive issues arising are discussed at IT Committee meetings.	**7.35.3** - For a sample of providers, review of the service reports confirmed partner oversight at least annually of the service including any actions arising as needed. No exceptions noted.

Information technology (Managing and monitoring compliance and outsourcing)

The services provided by Subservice Organisations are regularly monitored and assessed against the standards set out in the service level agreements

Process description

Some IT services and activities are outsourced to third parties. The partner responsible for overseeing the relationship with the Critical Supplier ensures regular monitoring of the outsourced service.

Control activity	Auditor testing
7.36 - Regular service reports are submitted by the network service provider against pre agreed service level objectives. Reports are reviewed by the Head of IT Operations and any issues arising are discussed at IT Committee meetings.	**7.36** - A sample of service reports were confirmed by observation and were provided by the Head of IT Operations. No exceptions noted.

Glossary

AAF	Audit and Assurance Faculty (of the Institute of Chartered Accountants in England and Wales).
API	Application Programming Interface.
Associate	Associate of Barnett Waddingham, part of the senior management team.
Authoriser	A pooled banking permissions group for authorising transactions, comprising experienced pension administrators and Pension Administration associates.
BWebstream	Barnett Waddingham's registration portal for members, trustees, HR/payroll teams and third-parties authorised by the trustees.
BWWord	Barnett Waddingham tool used to create and update the letters and statements available from Penstream.
Cashstream	Barnett Waddingham accounting software module within the Penstream software.
CCM	Client Cash Manager – a banking software solution from Cashfac PLC.
Client Account Manager	Staff member responsible for managing the relationship with a client or group of clients.
Client Relationship Manager	Pension Administration staff member responsible for managing the relationship with a client or group of clients.
Compliance Officer	Governance partner responsible for regulatory compliance matters.
DB	Defined Benefit, including final salary and Career Average Revalued Earnings (CARE) schemes.
DC	Defined Contribution, sometimes referred to as Money Purchase (MP).
Developer	IT software programmer.
Development Team Leader	Staff member responsible for management of a team of IT developers.
DPS	Data Provisioning Service, an interface used by HMRC to electronically deliver notices in respect of payroll pensioners.
eChecklist	Electronic checklist containing a list and audit trail of steps for repetitive tasks.
Gatekeeper	A pooled banking permissions group for authorising transactions, comprising Pension Administration partners and principals.

Head of Software Development	Staff member responsible for the management of a group of software development staff.
HMRC	HM Revenue & Customs.
HTTPS	Hypertext Transfer Protocol Secure, a combination of the Hypertext Transfer Protocol with the SSL/TLS protocol to provide encrypted communication.
ISAE 3402	International Standard on Assurance Engagements (ISAE) 3402 is a global assurance standard for reporting on controls issued by the International Auditing and Assurance Standards Board (IAASB).
Information Security Manager	Governance staff member responsible for setting appropriate Information Security policy, procedures and controls.
IT	Information Technology.
IT Committee	Team of senior personnel responsible for overseeing the management of Barnett Waddingham's IT infrastructure.
IT Team Leader	Staff member responsible for management of team of IT staff.
Network Administrator	Network operations and IT support team staff with elevated network domain access privileges to maintain Barnett Waddingham's IT infrastructure and network.
PAB	Pension Administration Board – comprises Pension Administration partners who oversee strategic management of the Pension Administration Business Area.
PAPG	Pension Administration Planning Group – comprises the Pension Administration senior management team who oversee the implementation of strategy determined by the PAB.
Partner	Partner of Barnett Waddingham, part of the senior management team.
PAYE	Pay As You Earn.
Payroll Administrator	Authorised staff member responsible for administering Bacs payments and centralised payroll and financial functions.
Pension Accounts Group Technical Committee	This group monitors regulatory and legislative developments in scheme accounting, including best practice in accounting standards and leads the development of Barnett Waddingham processes to accommodate these.
Pension Systems Analyst	Skilled technical staff responsible for the set up and maintenance of schemes on Penstream.
Penstream	A collective term for the suite of Barnett Waddingham software solutions developed for pension administration, accounting, payroll and other services.

Penstream Product Owner	Responsible for managing the Penstream product backlog as well as maximising the value of and prioritising the work of the Penstream Development Team.
PIN	Personal Identification Number.
PPF	Pension Protection Fund.
PRCC	Professional, Risk and Compliance Committee - overseeing risk management in Barnett Waddingham, including data protection, information resources and compliance strategy.
Principal	Principal of Barnett Waddingham, part of the senior management team.
Procedural Guidance	Administration procedures and guidance on Barnett Waddingham's intranet, maintained by the Pension Administration Technical Team.
Project manager	Pension Administration Project Manager or Staff member responsible for overseeing the installation of a new client in the absence of a local dedicated Pension Administration Project Manager or Partner responsible for overseeing the development of Penstream.
Project Planning Lead	System architect (senior IT software programmer).
Quality Assurance Analyst	Pension Administration staff member responsible for performing root cause analysis on incidents logged to the Administration Feedback database.
Scheme Actuary	Named actuary appointed to advise the trustees of an occupational pension scheme.
Service Auditor	Independent practitioner appointed to provide an assurance opinion over the controls in this report.
SFX	Secure File Exchange, an online tool to facilitate the transmission of electronic files over HTTPS secure channels using logon and password credentials.
SORP	Statement Of Recommended Practice (Financial Reports of Pension Schemes).
SSL	Secure Sockets Layer, a cryptographic protocol providing communications security over the internet.
STP	Straight-through processing, an electronic communication protocol to standardise the transmission of investment transaction information.
STP System Administrator	Authorised administrator with elevated access privileges able to amend the STP system configuration.

Taskstream	Barnett Waddingham software used for work management, time recording and billing.
Taskstream Administrator	Taskstream authorisation level allowing additional user privileges.
Team Leader	Staff member responsible for management of group of staff.
Ticket system	A threaded conversational task management database accessible via web browser and email.
TLS	Transport Layer Security, a cryptographic protocol providing communications security over the internet.
TPR	The Pensions Regulator.
UaG	Users and Groups is Barnett Waddingham’s user group management software which is used to manage specific application permissions for collections, or teams of users.
UPS	Uninterruptible Power Supply.
USB	Universal Serial Bus (a common type of computer connection).
User Entity	Clients using our pension administration services.

Appendix A - Statement by Service Auditor

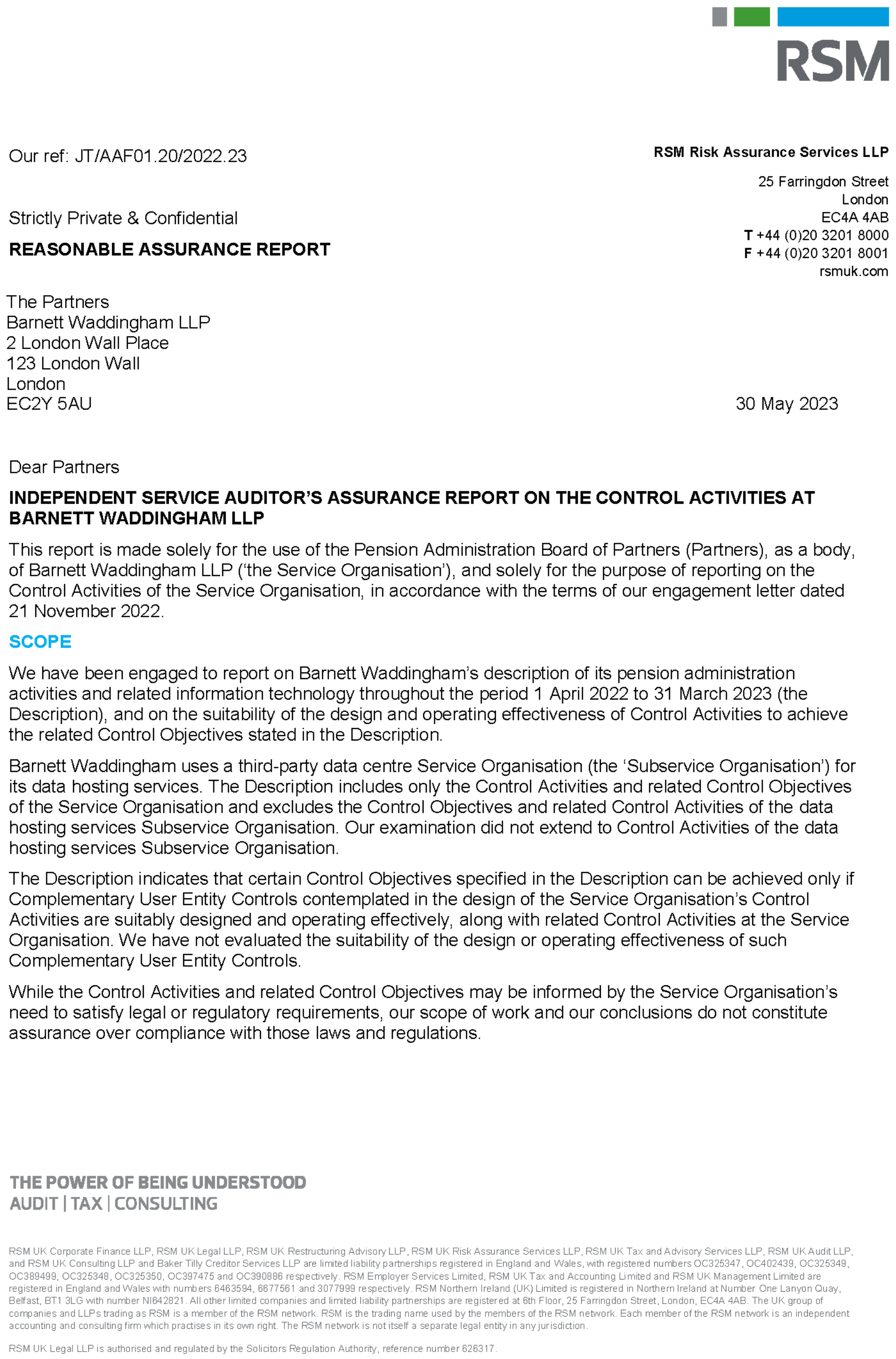
The Service Auditor’s Report, as set out at pages 126 to 128, has been prepared solely in accordance with terms of engagement agreed by the Pension Administration Board of Partners of Barnett Waddingham LLP (‘the Partners’) with RSM UK Risk Assurance Services LLP (‘the Service Auditor’) and for the confidential use of Barnett Waddingham LLP (‘the Service Organisation’) and solely for the purpose reporting on the Control Activities in providing an independent conclusion on the Partners' Statement set out at pages 20 to 21 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 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 a report by Service Auditors has been commissioned by the Partners of the Service Organisation and issued in connection with the 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 UK 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.

Appendix B – Report by the Service Auditor



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/AAF01.20/2022.23

Strictly Private & Confidential

REASONABLE ASSURANCE REPORT

The Partners
Barnett Waddingham LLP
2 London Wall Place
123 London Wall
London
EC2Y 5AU

30 May 2023

Dear Partners

INDEPENDENT SERVICE AUDITOR'S ASSURANCE REPORT ON THE CONTROL ACTIVITIES AT BARNETT WADDINGHAM LLP

This report is made solely for the use of the Pension Administration Board of Partners (Partners), as a body, of Barnett Waddingham LLP ('the Service Organisation'), and solely for the purpose of reporting on the Control Activities of the Service Organisation, in accordance with the terms of our engagement letter dated 21 November 2022.

SCOPE

We have been engaged to report on Barnett Waddingham's description of its pension administration activities and related information technology throughout the period 1 April 2022 to 31 March 2023 (the Description), and on the suitability of the design and operating effectiveness of Control Activities to achieve the related Control Objectives stated in the Description.

Barnett Waddingham uses a third-party data centre Service Organisation (the 'Subservice Organisation') for its data hosting services. The Description includes only the Control Activities and related Control Objectives of the Service Organisation and excludes the Control Objectives and related Control Activities of the data hosting services Subservice Organisation. Our examination did not extend to Control Activities of the data hosting services Subservice Organisation.

The Description indicates that certain Control Objectives specified in the Description can be achieved only if Complementary User Entity Controls contemplated in the design of the Service Organisation's Control Activities are suitably designed and operating effectively, along with related Control Activities at the Service Organisation. We have not evaluated the suitability of the design or operating effectiveness of such Complementary User Entity Controls.

While the Control Activities and related Control Objectives may be informed by the Service Organisation's need to satisfy legal or regulatory requirements, our scope of work and our conclusions do not constitute assurance over compliance with those laws and regulations.

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

USE OF SERVICE AUDITOR'S REPORT

Our work has been undertaken so that we might report to the Partners 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 current and prospective customers of the Service Organisation using the Service Organisation's pension administration services and related information technology ('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 the Partners of the Service Organisation and issued in connection with the Control Activities of the Service Organisation without assuming or accepting any responsibility or liability to them on our part.

SERVICE ORGANISATION'S RESPONSIBILITIES

The Service Organisation is responsible for:

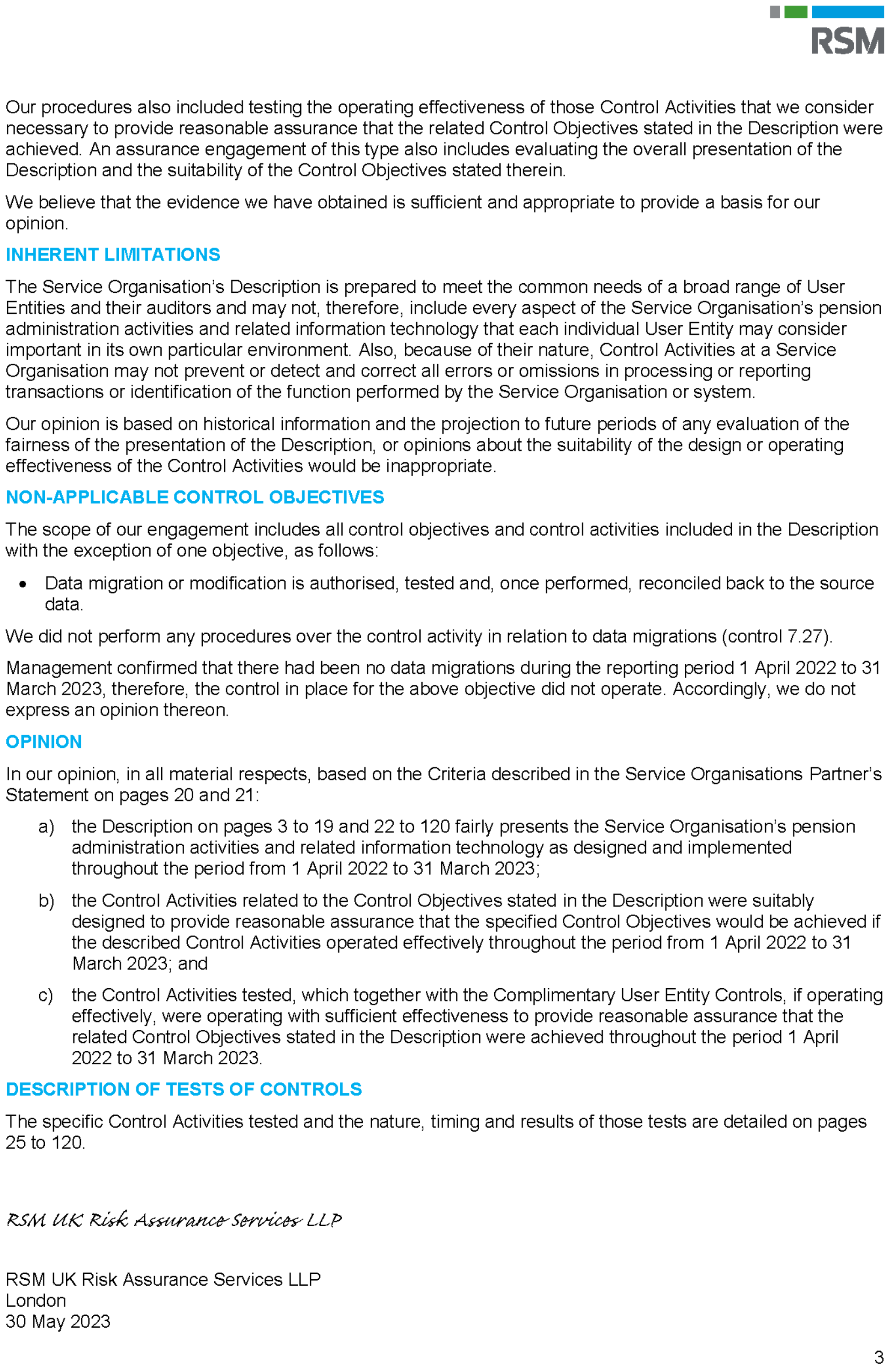
- preparing the Description on pages 3 to 19 and 22 to 120 and the accompanying Partners Statement set out on pages 20 and 21, including the completeness, accuracy, and method of presentation of the Description and the Management Statement;
- providing the Service Organisation's pension administration activities and related information technology 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, and effectively operating the Control Activities to achieve the stated Control Objectives.

The Control Objectives stated in the Description on pages 22 and 23, include the internal Control Objectives developed for the pension administration services and related information technology as set out in the ICAEW Technical Release AAF 01/20.

SERVICE AUDITOR'S RESPONSIBILITIES

Our responsibility is to express an opinion on the fairness of the presentation of the Description and on the suitability of the design and operating effectiveness of the Control Activities 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 (Revised), 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.

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 on pages 22 and 23. Our work involved performing procedures to obtain evidence about the presentation of the Description of the Service Organisation pension administration activities and related information technology and the design and operating effectiveness of those Control Activities. 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 Control Activities 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.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

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's pension administration activities and related information technology 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 objective, as follows:

- Data migration or modification is authorised, tested and, once performed, reconciled back to the source data.

We did not perform any procedures over the control activity in relation to data migrations (control 7.27).

Management confirmed that there had been no data migrations during the reporting period 1 April 2022 to 31 March 2023, therefore, the control in place for the above objective did not operate. Accordingly, we do not express an opinion thereon.

OPINION

In our opinion, in all material respects, based on the Criteria described in the Service Organisations Partner's Statement on pages 20 and 21:

a) the Description on pages 3 to 19 and 22 to 120 fairly presents the Service Organisation's pension administration activities and related information technology as designed and implemented throughout the period from 1 April 2022 to 31 March 2023;

b) the Control Activities related to the Control Objectives stated in the Description 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 April 2022 to 31 March 2023; and

c) the Control Activities tested, which together with the Complimentary User Entity Controls, if operating effectively, were operating with sufficient effectiveness to provide reasonable assurance that the related Control Objectives stated in the Description were achieved throughout the period 1 April 2022 to 31 March 2023.

DESCRIPTION OF TESTS OF CONTROLS

The specific Control Activities tested and the nature, timing and results of those tests are detailed on pages 25 to 120.

RSM UK Risk Assurance Services LLP

RSM UK Risk Assurance Services LLP
London
30 May 2023

Appendix C – Service Auditors' Engagement Letter

RSM

RSM UK Risk Assurance Services LLP

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

Our ref: JT/AAF0120/2022.23
Your ref:

21 November 2022

Strictly Private & Confidential

The Partners
Barnett Waddingham LLP
2 London Wall Place
123 London Wall
London
EC2Y 5AU

To the Partners of Barnett Waddingham LLP,

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 Audit and Assurance Faculty Technical Release 01/20 (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 December 2021.

RESPONSIBILITIES OF PARTNERS

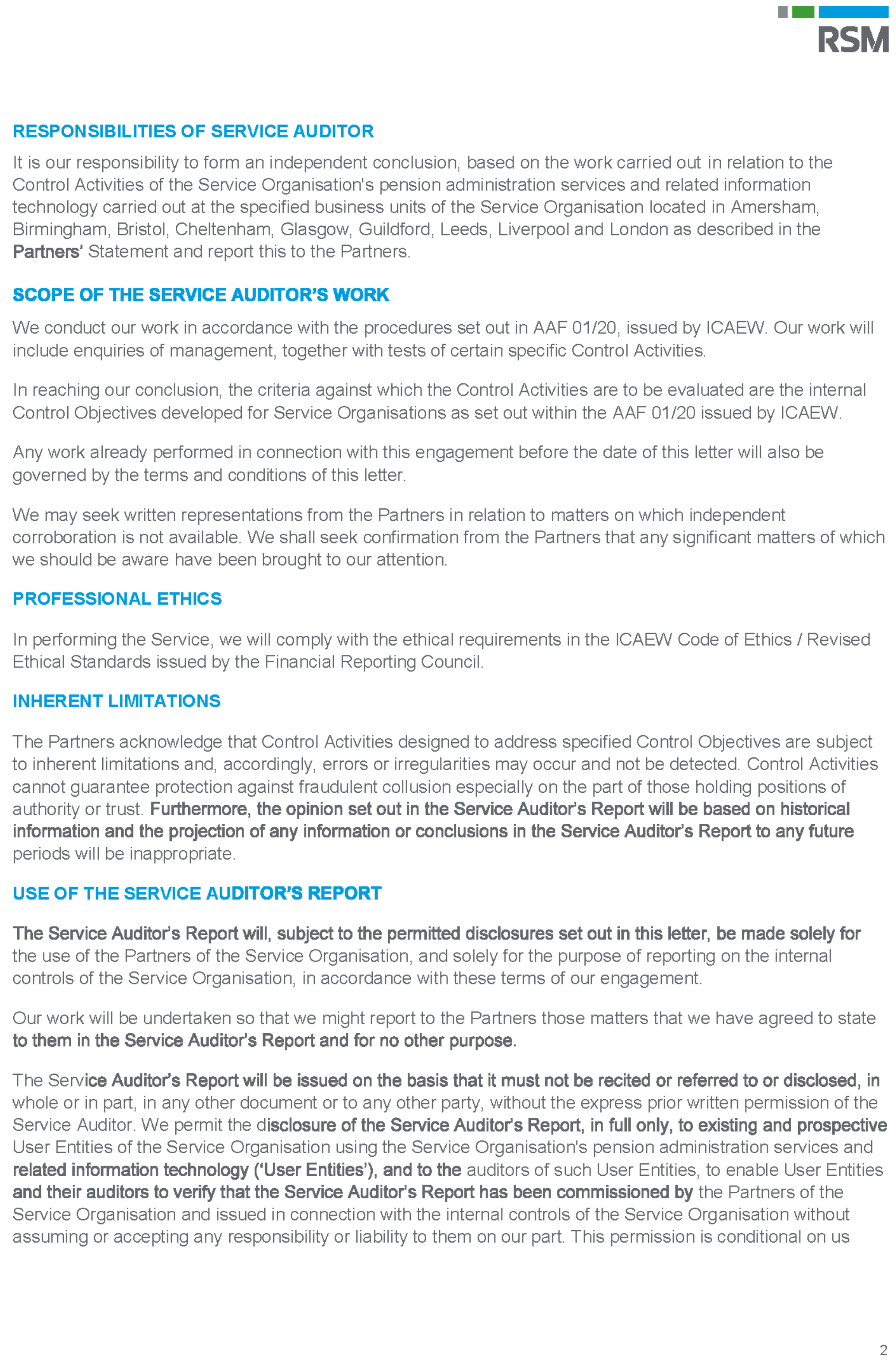
The **Pension Administration Board of Partners ("the Partners") of Barnett Waddingham LLP ('Service Organisation') in relation to which the Service Auditors report is to be provided, are and shall be responsible for** the design, implementation and operation of Control Activities that provide adequate level of control over pension administration services and related information technology. The Partners 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 ('**Partners **Statement') of the effectiveness of the Service Organisation's internal** controls for the relevant reporting period.

In drafting this report, the Partners 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.

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, RSM UK Consulting LLP and RSM UK Creditor Solutions LLP are limited liability partnerships registered in England and Wales, with registered numbers OC325347, OC402439, OC325349, OC389499, OC325348, OC325350, OC397475 and OC390886 respectively. RSM UK 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.



RSM

RESPONSIBILITIES OF SERVICE AUDITOR

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 pension administration services and related information technology carried out at the specified business units of the Service Organisation located in Amersham, Birmingham, Bristol, Cheltenham, Glasgow, Guildford, Leeds, Liverpool and London as described in the **Partners'** Statement and report this to the Partners.

SCOPE OF THE SERVICE AUDITOR'S 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 the Partners in relation to matters on which independent corroboration is not available. We shall seek confirmation from the Partners that any significant matters of which we should be aware have been brought to our attention.

PROFESSIONAL ETHICS

In performing the Service, we will comply with the ethical requirements in the ICAEW Code of Ethics / Revised Ethical Standards issued by the Financial Reporting Council.

INHERENT LIMITATIONS

The Partners 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 Auditor's 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 AUDITOR'S REPORT

The Service Auditor's Report will, subject to the permitted disclosures set out in this letter, be made solely for the use of the Partners 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 the Partners those matters that we have agreed to state **to them in the Service Auditor's Report and for no other purpose.**

The Servi**ce 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 d**isclosure of the Service Auditor's Report, in full only, to existing and prospective** User Entities of the Service Organisation using the Service Organisation's pension administration services and **related information technology ('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** the Partners 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. This permission is conditional on us agreeing with you clarification wording (Appendix 2) to be included as an introduction and on the Service **Organisation's websi**te.

To the fullest extent permitted by law, we do not and will not accept or assume responsibility to anyone other than the Partners **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 our Report on the Service **Organisation's website,** subject to, prior to this, us agreeing with you the wording of the introduction to the report on your website. In addition this permission is granted only if the 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 Customers and their auditors to verify that a report by reporting accountants has been commissioned by the Partners of the Organisation and issued in connection with the internal controls of the 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 UK 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.**

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 Service Organisation agrees to indemnify and hold harmless RSM UK Risk Assurance Services LLP and its partners and staff against all actions, proceedings and claims brought or threatened against RSM UK Risk Assurance Services LLP or against any of its partners and staff by any persons other than the Senior Management as a body and the Service 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 UK Risk **Assurance Services LLP's work under this engagement letter.'**

AGREEMENT OF TERMS

Please confirm in writing your agreement to these terms by countersigning this letter. Where Adobe Sign or similar is not used to countersign, please return a signed copy of this letter to us by another means.

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 UK Risk Assurance Services LLP

RSM UK Risk Assurance Services LLP

Encs. Terms and Conditions of Business dated December 2021

Contents noted and agreed for and on behalf of Barnett Waddingham LLP

Signed Paul Latimer ………………………… Date 09/12/2022 …………………………

AUTHORISED SIGNATORY

BARNETT WADDINGHAM

beyond the expected

Please speak to your Barnett Waddingham contact if you would like to discuss this report in more detail. Alternatively contact us via the following:

paul.latimer@barnett-waddingham.co.uk	01494 788134
richard.goddard@barnett-waddingham.co.uk	01242 548590

www.barnett-waddingham.co.uk