PENSION ADMINISTRATION

Assurance Report on Internal Controls

AAF 01/20 and ISAE 3402 Type 2 report for the period

1 April 2025 to 31 March 2026

BARNETT WADDINGHAM

Part of HOWDEN

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 and related information technology 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.

This report covers the period from 1 April 2025 to 31 March 2026 and contains an independent opinion on the operating effectiveness, as well as the existence and effectiveness of design, of our control procedures.

"At Barnett Waddingham, we believe our assurance report reflects the highest standards of reporting in the industry. We take great pride in our PASA accreditation, Investor in Customers Gold Award, Cyber Essentials and Cyber Essentials Plus certifications, as well as our ISO 27001 and ISO 9001 qualifications. These recognitions are a testament to the strength of our control environment and our unwavering commitment to delivering exceptional, secure and customer-focused services."

PAUL LATIMER
Partner and Head of Pension Administration – Barnett Waddingham

Our Pension Administration Internal Controls team

Responsibility for the oversight of procedures and internal controls sits with Paul Latimer, Head of Pension Administration. The ongoing maintenance and monitoring of the control environment is undertaken by the Pension Administration Internal Controls team, which forms part of the Operational Assurance function area led by Richard Goddard.

During the reporting period, Philippa Wardman and Chris Flanagan from the Internal Controls team oversaw the coordination of the annual independent audit of our internal controls. The team supported the Service Auditors throughout the process, ensuring they had timely access to relevant systems, documentation and subject-matter experts. Their work helps to ensure that our control framework remains robust and operates effectively.

About us

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

With a team of more than 1,700 people across eleven offices, we work to deliver exceptional service through our commitment to trust, integrity, and quality.

We are a trusted partner for a wide range of clients in both the private and public sectors – this includes 24% of FTSE 100 and more than 15% of FTSE 350 companies.

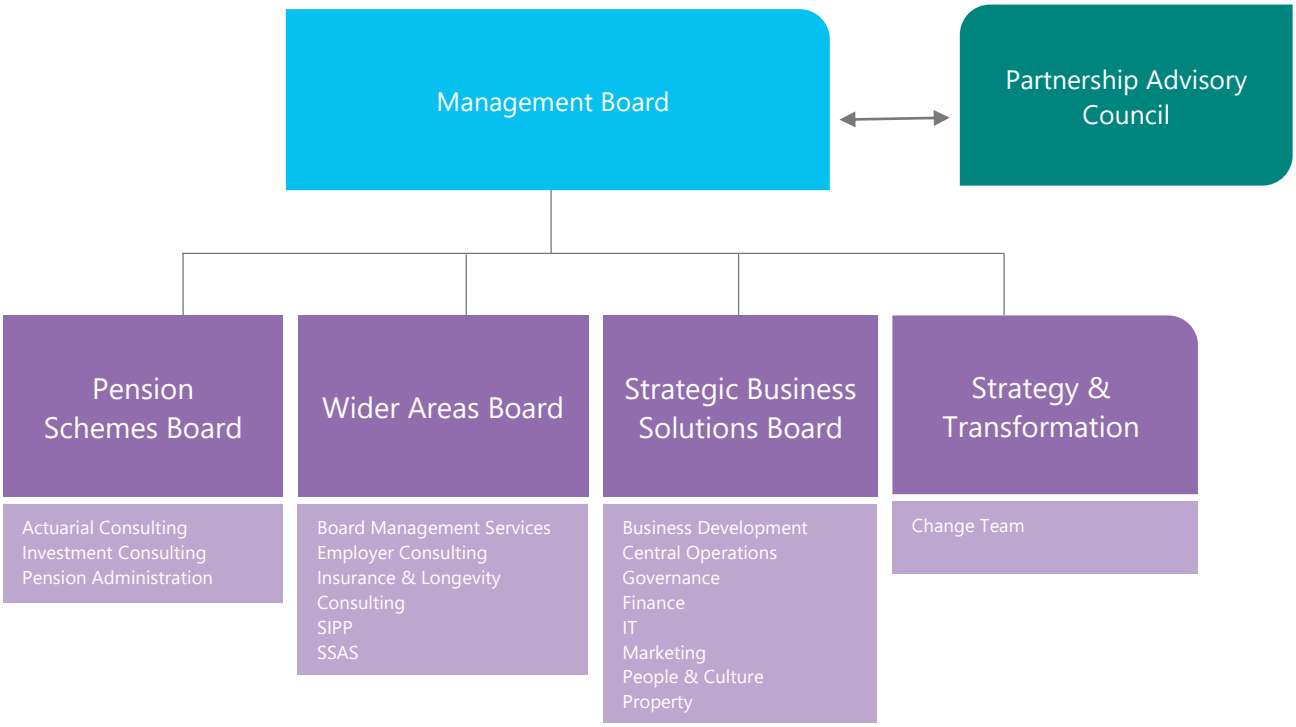
We leverage our deep expertise to bring innovative solutions, ensuring long-term value for our clients through strategic insights and dedicated partnership.

During December 2025, we opened an office in the heart of Edinburgh continuing our ambitious trajectory of growth and reaffirming our commitment to clients in Scotland.

We confirmed the completion of the acquisition of Barnett Waddingham by Howden, a global insurance and employee benefits intermediary group, on 3 April 2025. This creates one of the largest pensions and employee benefits firms in the UK.

Barnett Waddingham continues to operate as part of the Howden Group. Integration between the two organisations is ongoing, with several teams now working within shared governance and leadership structures. Over time, there may be changes to how the business presents its external brand and materials, reflecting its position within the Howden Group. Any such changes would be managed carefully and communicated separately.

The following diagram shows the operational structure of Barnett Waddingham as at 31 March 2026:



Our purpose

We empower people to secure better futures.

To achieve this, we foster strong relationships by communicating transparently, supporting growth, and championing diverse perspectives with respect and kindness. Our resolve for finding solutions sees us continually exploring new ideas, addressing challenges directly, and leveraging our collective expertise to drive excellence. We deliver proven impactful results by honouring commitments, striving for excellence, and embracing smart risks that propel us and our clients forward.

Our people

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 employees have a depth of consulting expertise and a breadth of administrative skills, supported by the latest technology that allows us to tackle a wide range of work – from advising small clients to dealing with large pension schemes and employers.

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.

Pension Administration

Our experienced and professional pension administration team provides services to c.400 clients comprising c.420,000 members and policyholders; covering defined benefit (DB), defined contribution (DC), hybrid, Career Average Related Earnings (CARE), open, closed, insurance administration, consolidator administration, and those transferring to the Pension Protection Fund (PPF).

Our administration services are provided by dedicated teams supported by our specialist groups covering systems, accounts, projects and communications. Our staff work collaboratively, with all our offices using the same systems and procedures to make things seamless and straightforward for our clients.

Administration

- Membership record-keeping.
- Benefit calculations and payments, including electronic payments.
- All regulatory reporting.
- Full cash and accounting services, including drafting the annual report and accounts and pooled banking facilities.
- Pensioner payroll.
- Member helplines.
- Member tracing and pensioner existence.

Specialist administration

- Data gap analysis, data verification and data cleansing.
- Benefit audits.
- Benefit rectifications, including Guaranteed Minimum Pension (GMP) projects.
- Pensions Dashboards preparation.
- Journey to endgame.

Transaction data readiness

As insurers get busier, they're looking carefully at the level of preparation work that schemes have carried out and they are keen to engage with schemes that can demonstrate the necessary level of commitment to a transaction.

We're experts in supporting trustees and scheme sponsors on their scheme's data journey. We understand the steps required to prepare the scheme for a transaction. We can undertake all aspects of the data preparation work – this can be included alongside other services or on a standalone project basis. Our services include:

- Data gap analysis with comprehensive reporting and tailored recommendations, targeting best insurer pricing.
- All aspects of data cleanse work and planning to meet transaction objectives.
- Targeted benefit audit.
- Data verification exercise to check data with members.
- Obtaining marital status and contingent spouse data.
- Member tracing and mortality screening.

PPF administration

We're one of the four members of the PPF's Specialist Administration and Actuarial Services Panel. We provide administration to schemes entering a PPF assessment period and prepare them for transfer to the PPF. Our services include:

- Member helplines to support members after the insolvency of their employer.
- Pensioner payroll, ensuring continuity of service at the point of insolvency.
- Member calculations in line with PPF legislation.
- Member announcements and bespoke communications.
- Data verification with members.
- Data audit and rectification.
- Benefit audit and rectification.
- Member tracing and pensioner existence.
- Preparation of valuation data and scheme accounts.
- Transfer of underfunded schemes to the PPF.
- Comprehensive preparation for buyout for schemes that are funded above PPF levels.

We also carry the PPF Trustmark. This is in recognition of our collaborative work with the PPF and specialist knowledge. It reassures members and other scheme stakeholders of our commitment to delivering the high standards expected by the PPF.

"Our administration proposition is built on offering a quality service to our clients for every part of their pensions journey, and for every challenge coming along the regulatory pipeline. We are incredibly proud of our dedicated team of professional administrators who continue to support all our clients and members."

ANDY GREIG
Partner and Head of Pension Administration Client Management – Barnett Waddingham

Pension Administration Partners and Heads of Function

For the company year beginning 1 June 2025, there were 11 Pension Administration Partners.

The Pension Administration Heads of Function, who consist primarily of Partners, set the high-level priorities, targets and goals for the Pension Administration business area. They report via Paul Latimer, Head of Pension Administration, who represents the business area to the Pension Schemes Board.

Head of Pension Administration, Business Area Leader

Paul Latimer, Partner

Client

Head of Pension Administration Client Management

Andy Greig
Partner

Head of Pension Administration Proposition

Amanda Bradley
Partner

Head of Pension Administration Business Development

Chris Tagg
Partner

Head of Pension Administration Client Relationship Management

Collette Graham
Partner

Head of Pension Administration Pricing and Technical

Julian Mainwood
Partner

Head of Pension Administration Marketing and Bid

Sharon Khan
Partner

People

Head of Pension Administration People

Fiona Rumsby
Partner

Finance

Head of Pension Administration Finance

Paula Hendry
Partner

Operations

Head of Pension Administration Technology

Ben Clacker
Partner

Head of Future Ready and Pension Administration Operations Management

Emer Gracie

Head of Pension Administration Operational Support

Heather Peters
Principal

Head of Pension Administration Operational Delivery

Tom Cowley
Partner

Function Area Leaders

Function Area Leaders are responsible for ensuring their areas within Pension Administration operate effectively and in line with overall business objectives. They report into the relevant Head of Function and act as day-to-day decision makers for their teams, focusing on efficient delivery, commercial awareness, regulatory compliance, and maintaining strong client service standards.

As senior representatives of their function areas, they monitor performance, manage risks and issues, and work with colleagues to resolve cross-functional challenges. Through this structured oversight and their accountability to Heads of Function, the group helps maintain consistent, well-governed, and high-quality service delivery for clients.

Operations managers and consultants

Function Area Leaders are supported by operations managers and consultants, who provide the operational and technical expertise needed to deliver the function area's objectives. Operations managers oversee the day-to-day running of teams, ensuring services are delivered efficiently, accurately, and in line with the business area's strategic priorities. They help translate functional strategies into practical delivery plans, manage team performance, and maintain high standards of client service and regulatory compliance.

Consultants complement this by offering specialist technical expertise. They support leaders and operations managers by developing technical solutions, advising on complex cases, and ensuring that the services delivered by the team meet required industry standards. Their insight helps drive innovation, maintain accuracy, and identify opportunities for improvement or risk mitigation.

Pension administration teams

Our administration teams consist of pension administrators with a full range of experience and skills 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 teams

Alongside the pension administration teams there are several specialist teams who provide either local support or centralised firmwide 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.

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.

"Achieving PASA accreditation is a challenging process, and we are thrilled that our unwavering commitment to providing the highest quality services to UK pension schemes and their members is recognised in this way. Moreover, Barnett Waddingham has continued to go through the re-accreditation every three years, further demonstrating our dedication to excellence in administration."

PAUL LATIMER
Partner and Head of Pension Administration

PMI Insight Partner and Development 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.

In November 2025, Barnett Waddingham became a founding Development Partner in the PMI's Development Partnerships Programme, supporting the PMI's commitment to raising professional standards.

"The PMI plays a vital role in raising standards across our profession, so we're proud to be a founding Development Partner in this initiative. At Barnett Waddingham we've always believed that long-term investment in people, skills and qualifications is essential to delivering the best outcomes for pension schemes and their members. We look forward to working with the PMI and other partners to strengthen professional development right across the sector."

NICK WALKER
Principal and Senior Operations Manager for Training, Pension Administration – Barnett Waddingham

Future developments

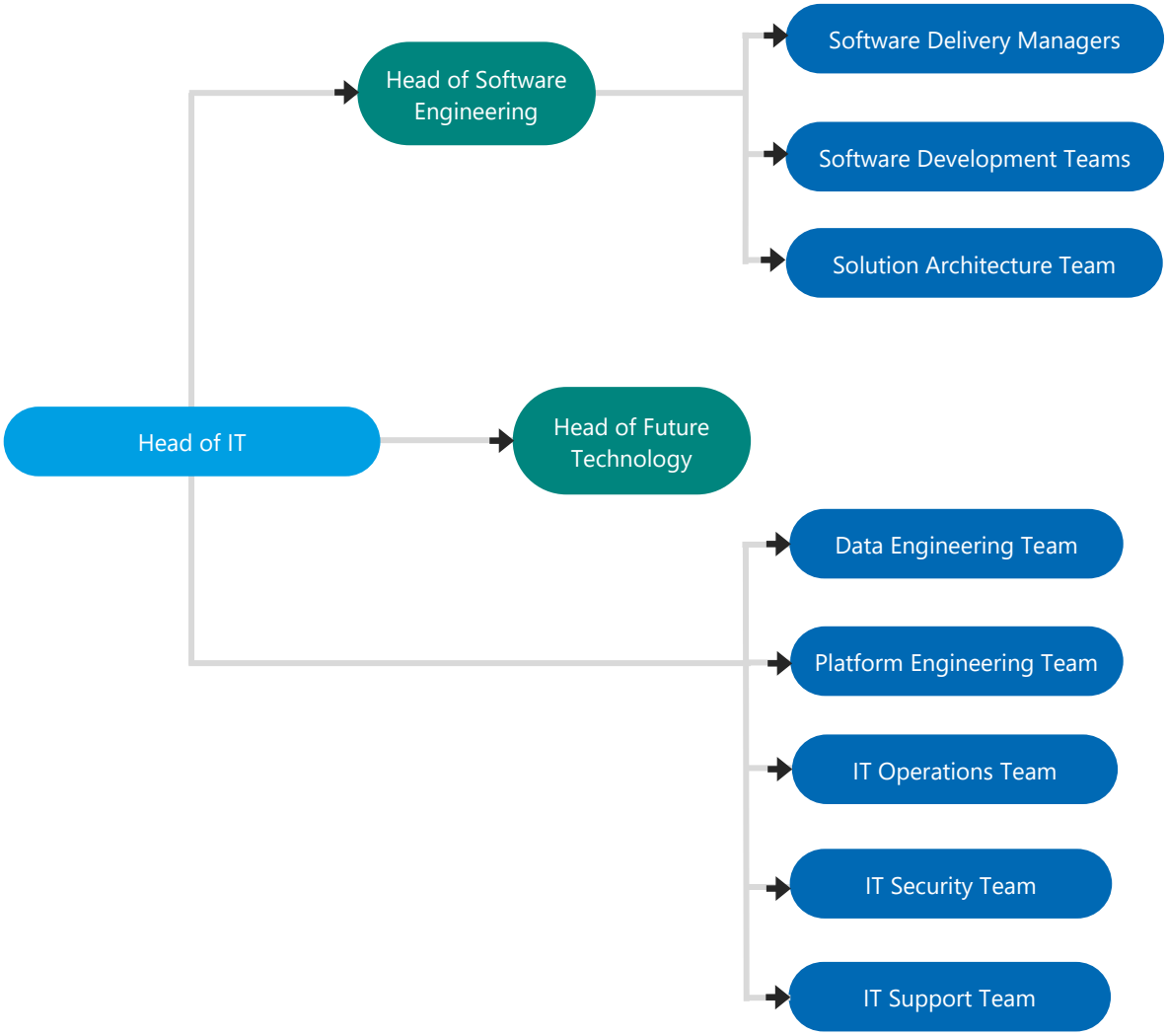
We're proud of the strong partnerships we've built with our clients and the consistent, high-quality pension administration service they can expect from us. Our business has grown significantly over the last decade, and, throughout this time, we have continually looked at ways to improve the services we offer to our clients, as well as providing continued opportunities for our people. We have invested year on year in system development, training and enhancing our services for our clients.

The pension administration landscape is now changing, this is bringing with it a demand for more varied services and specialisms, and increased member expectations. We have listened to our clients, their members, and our people. In response to this, we are refreshing the way we operate – how we organise ourselves and how our pension administration teams are structured and supported. This will help ensure we have a sustainable business that can meet the needs of our clients and our people. We call this FutureReady.

FutureReady ensures we have the right people, doing the right work, at the right time, harnessing new and improved technology. Continuous improvement will remain at the core of our operation. This will ensure we stay responsive, consistent, and efficient as we grow and develop our business.

Information Technology (IT)

The Head of IT decides high-level priorities, targets and goals for the IT Team and reports to the Strategic Business Solutions Board.



IT Committee

The role of the IT Committee is to support the Head of IT in fulfilling their accountabilities and in particular to challenge plans to ensure they are fully thought through and robust. Implementation can be as important as the activity itself and it is the committee's job to consider how activity will be received and the best way to influence colleagues effectively.

The committee is chaired by the Head of IT and comprises representatives from both within the IT Team and from other business areas, including the Head of Pension Administration Technology.

The committee meets quarterly to discuss high-level strategic direction and project progress and meet monthly to discuss operational matters.

Pension Administration Software

Penstream

Our proprietary administration system, Penstream, is used for day-to-day administration, record-keeping, contribution processing, benefit calculations and administering of DB, DC and CARE pension data. It is fully integrated with Taskstream for workflow management and with Cashstream, which is used for accounts and treasury.

Investment process automation is supported on Penstream using a Straight-Through Processing (STP) funds trading automation product that provides pension fund trading and automation of fund price and holding feeds.

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. The pension payroll function provides integrated net pay and tax calculations and reports. Internet technology is at the heart of Penstream payroll; our system fully supports PAYE Real Time Information (RTI) and communicates seamlessly with the HMRC Online Services over the internet.

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 accounting module – Cashstream. For accounting purposes, Cashstream automatically records payments generated by administrators using Penstream. For clients using our pooled bank account, Cashstream generates payment instructions against the relevant segregated account where authorisation transaction limits are automatically enforced, ensuring a streamlined process.

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 management 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 which is programmed with administration service standards agreed with our clients.

Tasks are linked to member records and can hold an electronic checklist (eChecklist) which guides administrators through controlled processes.

eFiling is our electronic data management and document imaging system. eFiling is integrated with Penstream, Taskstream and Pension 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.

Clarity from BW

Clarity from BW is the gateway to the powerful technology suite that underpins our expert consultancy. Designed to help businesses thrive and support pension schemes with current and future objectives, our online tools provide sharper insights, address complex challenges, and allow decision-making with greater certainty.

Clarity provides access to three distinct categories, each tailored to meet the specific needs of the different client segments that Barnett Waddingham serves as a firm, not just for Pension Administration:

Clarity Analyse: designed to empower clients to make confident, well-informed decisions using their data. Key tools include Illuminate, GEM, and Insight, which provide deep analytics and actionable insights.

Clarity Connect: places individuals in control of their data with instant access to information in a secure self-service environment. Notable tools accessed in this category include 4me, and Pension self-service.

Clarity Control: aimed at increasing efficiency and minimising errors, this tranche aids compliance and saves both time and money.

Pension self-service

Pension self-service is just one of the services accessed from a Clarity from BW account.

Pension self-service is for members of the schemes that we administer. It has been designed with control and reassurance in mind, providing a one-stop location for all the important information members need to manage their retirement.

Users can access the latest communications, submit documents and dive deep into the various aspects of their pension. All of this is backed up by our wide-ranging security measures, put in place to give peace of mind to everyone.

System features include:

My homepage	A clear summary of all scheme benefits and payments, with simple navigation to help explore benefits in full, alongside easy access to the latest pension documents.
My name and greetings	Personalised greetings and communications.
My pension	View current benefit and retirement illustrations.
My service	Get an overview of key service dates, earnings and contributions.
Online identity check	Our online check provides a quick and efficient verification process, removing the need for sensitive documents to be sent to us in the post.
My payroll	View details of current payments, payments made, payslips and tax history.
My documents	Access to all pension documents in a single place, with the option to securely send documents digitally.

Insight

Insight, our online dashboard for trustees, is designed to make pension scheme analytics available to our clients, presented in a clear way that allows instant analysis.

Our Insight tool will:

- Provide on-demand secure access to a summary of a scheme's data.
- Allow clients to query data summaries, in their own time and with their own filters, so they can better understand their own data.
- Allow trustees and consultants to spot trends or other interesting features early, improving decision-making time.
- Provide better transparency, as all data is taken directly from our systems.
- Allow everyone to work with the same tool, leading to smoother and clearer communication between trustees and administrators.
- Enable queries to be answered outside of the normal meeting cycle, in particular questions that are not business as usual.

Insight's features and capabilities include:

- Volume of work and our performance measured against our service level agreement.
- The scheme's membership breakdown and the member movements over time.
- The age that members have been retiring, and the type of retirement they've taken.
- The age profile of the membership.
- Member online activity (e.g. number of members logging in to member websites).

Our integrated AI assistant is designed to help clients navigate and interpret their scheme's analytics dashboard more efficiently.

This intelligent tool responds to clients' queries about their data, providing clear guidance on where information can be found whilst maintaining the highest standards of data security and professionalism.

By combining instant responses with intelligent suggestions about data trends, the Insight Assistant allows clients to focus on strategic oversight rather than platform navigation, ultimately empowering smarter, member-focused decision-making.

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 ways.

Procedures

Procedures for controlled tasks are managed and maintained by delegated owners within either the Pension Administration section of our corporate SharePoint intranet, or Taskstream eChecklists. Procedures are version controlled to ensure an audit trail is maintained; and edit restrictions are used so that only authorised users can change content.

Procedural Guidance is an intranet-based manual of pension administration procedures for most controlled administration tasks which also holds technical information for pension administrators.

Communications

Pension Administration's 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

The quality of work is a core priority, and our aim is to ensure that tasks are completed correctly first time by individuals with the appropriate experience and expertise. While most tasks are reviewed for accuracy and reasonableness, there may be instances where such reviews are not required or are replaced by other controls, such as the use of pre-approved letter templates. This approach allows flexibility within our internal control framework, accommodating different scenarios while maintaining the integrity and quality of our processes.

Information security programme

ISO certification

Barnett Waddingham is proud to hold Quality Management (ISO 9001:2015) and Information Security Management (ISO 27001:2022) certifications. ISO international standards ensure that products and services are safe, reliable and of good quality.

One of the strengths of ISO standards is that they are created by the people that need them. Industry experts from over 170 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. We undergo annual audits by a UKAS-accredited ISO certification body and Barnett Waddingham conduct regular internal audits to ensure compliance with controls is maintained.

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.

Barnett Waddingham first achieved Cyber Essentials certification in 2019 and Cyber Essentials Plus in 2021 and is committed to retaining both certifications. We undergo annual assessments by an IASME-accredited certification body to ensure certification is retained.

Policy reviews

Firmwide information security and quality policies and procedures are subject to regular monitoring and annual reviews or after any significant technological change.

Personnel

Vetting

Barnett Waddingham carries out comprehensive vetting of all individuals prior to employment. The identity of all staff and agents who will have access to confidential information or will be involved in the development of any system code, is confirmed using verifiable identity documents prior to creating accounts which give access to confidential information or rights to commit code to our code repositories.

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

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, Ransomware, Identity Fraud and Staying Safe Online. This programme is delivered via different media including eLearning modules, intranet blogs, email, presentations and corporate communication tools.

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 is responsible for hosting data and uses a third-party data centre, the hosting site is rated Tier 3 and has comprehensive multi-layered physical site security in place. A Tier 3 data centre has multiple paths for power and cooling, with systems in place to allow maintenance and updates without taking it offline. It has an expected annual uptime of 99.9%. The data centre is protected against unauthorised access 24 hours a day, 365 days a year. The comprehensive physical site security measures include:

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

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

Clear desk and clear screen policy

We have implemented a clear desk and clear screen policy to ensure that no confidential information can be accessed inappropriately, for example, by out of hours cleaning staff. Screens automatically lock after 10 minutes of inactivity. Regular security sweeps are carried out to ensure this policy is followed and enforced.

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.
- 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.
- Delegated day to day oversight of our adherence to the ISMS to Barnett Waddingham's Data Protection and Information Security Oversight 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 anonymised 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 their role.

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.

Multi factor authentication

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

All users must verify their identity when prompted on each device. Once authenticated on the relevant device, applications and data will be accessible for a period determined by the user's role. Users with elevated privileges or administrative responsibilities are required to re-authenticate more frequently. Access to all Office 365 services remains blocked until re-authentication has been successfully completed.

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.

Certificates

Certificates used on externally facing Barnett Waddingham websites are provided by a third-party certificate authority.

For certificates required internally, we operate our own certificate infrastructure. These certificates are typically used for application code signing and access management. The private keys used in these cases are securely managed in our public key infrastructure and access is regularly reviewed.

Key management

Our key management is based on an External Key Management (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.

Data retention

Retention periods

Barnett Waddingham's data retention policy regarding customer and/or supplier data (summarised below) has been designed to meet legal, fiscal and regulatory requirements.

Indefinite	• Documentation relating to pension transfer, pension opt-out or FSAVC advice. • Complaints and incidents records.
Seven years (unless otherwise agreed)	• All other customer related documents.

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 drives, CDs, removable storage drives and imaging equipment is securely destroyed. This is achieved by physically removing the storage media and ensuring its destruction by CESG approved third parties who provide certificates of destruction. Where physical removal is not possible, data is securely wiped using appropriate tools.

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 AES 256-bit, 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), version 1.2 or higher. For transferring data files, our secure communication services should be used.

Secure File Exchange (SFX)

Secure File Exchange (SFX) is an online service provided by Barnett Waddingham for sending and receiving files securely. 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

Barnett Waddingham hosts all personal data in the UK/EEA, unless specifically authorised by the client in advance, or otherwise to ensure we comply with our obligations under data protection laws.

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.

In addition to the email gateway, we utilise an advanced AI based analysis tool to scan all incoming emails for advanced threats including business email compromise (BEC), vendor fraud and account take-over. Suspicious emails are either deleted or quarantined depending on the risk level they pose. Staff receive regular training on how to identify and report these types of emails.

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 Clarity from BW portal is the front-door to our member and 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. Our systems also go through Dynamic Application Security Testing (DAST) and Static Application Security Testing (SAST) prior to release.

Device security

Build standards

Our servers and laptops are built using security tested standard images. We carry out regular vulnerability scans on all assets 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 mitigate the risk of malware infections, 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 24/7 by an external Security Operations Centre (SOC), who are able to interpret and react to alerts raised by the system. Events requiring attention are escalated to the IT Security team for investigation and response, with support from the IT Support team where remediation or technical assistance is required.

We have a documented policy and standard procedures for dealing with suspected and actual security events, incidents and cyber-attacks. All incidents are logged in an incident 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 exfiltrated.

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

Security logs are retained for a period of 12 months.

Business continuity

Backup 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 seven 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.

Backup 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 seven years.

Various backup data sets are tested monthly.

Business continuity and disaster recovery testing

Our business continuity plan and disaster recovery plan are tested at least once a year. We can recover mission critical systems within three hours, business critical systems within six hours and business desirable systems within nine to 12 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 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 2025 to 31 March 2026. 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;
- 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 2025 to 31 March 2026. 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;
- 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.

Paul Latimer

Paul Latimer
On behalf of the Pension Administration Partners, Barnett Waddingham LLP
27 May 2026

Control Objectives

Control objectives for pension administration services

(1) 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.

(2) 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.

(3) 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.

(4) 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.

(5) Managing and monitoring compliance and outsourcing

- Receipt 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.

(6) Reporting to clients

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

Control objectives for related information technology services

(7) 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.

(8) 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.

(9) 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.

(10) 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.

(11) 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 been 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.

The following table shows the services provided by Subservice Organisations used by Barnett Waddingham and the corresponding controls in this report which are involved.

Control Objective	Control	Service
Data received from external parties is scanned for known vulnerabilities, any compromised data is quarantined, and definitions of threats are periodically updated.	8.07.2 and 8.07.3	Cloud based email management, including security, archiving and continuity services
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.	8.09	Cloud workload and endpoint security, threat intelligence, and cyberattack response services
In-scope systems and data are backed up and tested such that they can be restored completely and within agreed timescales	10.02.3 and 10.02.4	Cloud backup and storage services

Controls 11.01.2 and 11.02 describe how we monitor outsourced activities.

Control Procedures and Service Auditor Tests

Summary of controls tested

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 figures 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			
(1) Accepting clients	3	8	0
(2) Authorising and processing transactions	3	22	0
(3) Maintaining financial and other records	4	18	0
(4) Safeguarding assets	2	16	0
(5) Managing and monitoring compliance and outsourcing	5	13	2
(6) Reporting to clients	2	6	0
Information Technology			
(7) Restricting access to systems and data	4	25	1
(8) Maintaining integrity of the systems	5	20	0
(9) Maintaining and developing systems hardware and software	3	8	0
(10) Recovering from processing interruptions	5	13	0
(11) Managing and monitoring compliance and outsourcing	2	3	0
TOTAL	**38**	**152**	**3**

Management response to exceptions

Management acknowledges the findings set out in the Service Auditor's report and remains committed to maintaining a robust and effective control environment. While the results of this year's engagement identified three minor exceptions, we note that these fall within the acceptable parameters defined by the AAF 01/20 framework and do not impact the overall achievement of the control objectives. Nonetheless, we recognise the importance of addressing all exceptions and have provided our response below to outline the context and actions taken.

Control 5.02

CONTROL ACTIVITY: Late contributions are reported by the pension administration team 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.

AUDITOR TESTING COMMENT: For a sample of late contributions, confirmed that the late contributions have been reported by the pension administration team to the Partner and followed up on.

In one instance it was noted that a backdated pension contribution was paid late (by one day) and the breach was not reported to the Partner in a timely manner.

MANAGEMENT RESPONSE: The audit finding relates to a pension contribution that was paid late and was not reported internally for assessment within the required timeframe. While the control framework for monitoring and assessing late contributions is established, this instance arose due to limitations in the visibility and tracking of late contribution reporting.

To address this, enhancements will be made to strengthen the monitoring of late contribution reporting. In addition, targeted refresher training will be provided to reinforce the internal reporting requirements for late contributions and breach assessment. These actions are intended to support consistent and timely identification and reporting of any future late contributions.

Control 5.10

CONTROL ACTIVITY: The annual HMRC Event Report completed by the pension administration team is reviewed for completeness and accuracy by a second pension administrator and the file is marked accordingly. Where Barnett Waddingham is engaged to submit the Event Report, client authorisation is obtained in advance of submission.

AUDITOR TESTING COMMENT: For a sample of HMRC Event Reports completed by the pension administration team, confirmed review by a second pension administrator. Where Barnett Waddingham is engaged to submit the Event Report, confirmed that client authorisation was obtained in advance of submission for the majority of the sample. Confirmed that the file was marked accordingly.

In two instances, however, there was no explicit evidence demonstrating that client authorisation had been obtained in advance of submission of the annual HMRC Event Report.

MANAGEMENT RESPONSE: The audit finding relates to instances where evidence of client authorisation prior to submission of the annual HMRC Event Report was not retained on file. While authorisation has been obtained, the supporting evidence was not consistently recorded at the point of submission.

To address this, the process will be strengthened to ensure that documented evidence of client authorisation is obtained and recorded as a required step prior to submission. Additional guidance and refresher training will also be provided to reinforce the importance of maintaining a complete and auditable record of approvals. These actions will support consistent retention of clear and verifiable evidence of authorisation.

Control 7.05.1

CONTROL ACTIVITY: Network access rights for new users and leavers are maintained by following either the onboarding or offboarding process and actions are recorded on the IT ticket system which is subject to review.

AUDITOR TESTING COMMENT: For a sample of new accounts, it was confirmed they were created by following the formal joiner's process with actions recorded in the IT ticket system.

For a sample of leavers, it was confirmed they were disabled by following the formal leaver's process with actions recorded in the IT ticket system.

It was noted, however, for a few of the leavers, the disabling of access was recorded after the leaving date. It was confirmed through last login dates that none of the leaver accounts were logged into after the leaving date.

MANAGEMENT RESPONSE: The audit finding relates to delays in recording the disabling of access for certain leaver accounts within the IT ticketing system. Testing confirmed that access had been removed and no accounts were accessed following the employees' leaving dates; however, the timing of the recorded evidence did not consistently demonstrate prompt execution of the control.

To address this, processes will be reinforced to ensure that both the removal of access and the recording of the action in the IT ticketing system are completed on a timely basis. Additional oversight will also be introduced to monitor the timeliness of these activities and ensure that a complete and accurate audit trail is consistently maintained.

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 comments
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, it was confirmed that the Engagement Letter had been signed by the Partner in charge of the client, evidencing approval of the Engagement Terms, including any client-specific customisation. 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, it was confirmed that the Engagement Letter had been signed by an authorised representative of the client prior to the commencement of services. No exceptions noted.

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 comments
1.02 – An Anti-Money Laundering verification review is completed for all clients other than those in a PPF assessment period before pension administration services begin. The review date and supporting information are recorded against the client record on Taskstream.	**1.02** – For a sample of clients, it was confirmed that an Anti-Money Laundering verification review had been completed prior to the commencement of pension administration services and that the review date and supporting information were recorded against the client record on Taskstream. No exceptions noted.

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 Administration clients the benefit specification is written by the appointed lawyers from the PPF panel. For Insurance Administration clients, the benefit specification is provided directly by the client.

Control activity	Auditor testing comments
1.03 – For Ongoing Administration 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 Ongoing Administration clients, it was confirmed that the benefit specification document had been prepared under the supervision of the project manager and retained on file, together with relevant validation correspondence with the client or their advisers. No exceptions noted.

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 the onboarding 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 Administration 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

1.04 – For Ongoing Administration and Insurance Administration clients a new client service project template or new client service tasks with eChecklists are added to Taskstream and progress is monitored 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.

Auditor testing comments

1.04 – For a sample of Ongoing Administration and Insurance Administration clients, it was confirmed that new client service project tasks were set up and monitored to completion in Taskstream, and that an end-of-project report had been produced by the project manager.

No exceptions noted.

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 comments
1.05.1 – For Ongoing Administration and Insurance Administration clients' data imported to Penstream is reconciled by the onboarding team to the source data which is retained indefinitely.	**1.05.1** – For a sample of Ongoing Administration and Insurance Administration clients, it was confirmed that data imported to Penstream had been reconciled to the source data by the onboarding team, with the source data retained on file. No exceptions noted.
1.05.2 – For Ongoing Administration and Insurance Administration clients the onboarding team record data reconciliation exceptions on the risk, action, issue and decision (RAID) log.	**1.05.2 –** For a sample of Ongoing Administration and Insurance Administration clients, it was confirmed that data reconciliation exceptions were recorded by the onboarding team on the risk, action, issue and decision (RAID) log. No exceptions noted.
1.05.3 – For Ongoing Administration and Insurance Administration 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 Ongoing Administration and Insurance Administration clients, it was confirmed that the risk, action, issue and decision (RAID) log was maintained by the project manager and that decisions made and actions taken were recorded on the log. No exceptions noted.

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 3.08 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 comments
2.01 – Penstream calculations generating the investment instruction are checked for accuracy with reference to the investment requirements. 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.	**2.01** – For a sample of schemes, it was confirmed that Penstream calculations generating investment instructions had been checked for accuracy against the investment requirements and that completion of the process had been recorded using an eChecklist. No exceptions noted.

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

For DC schemes, the pension administrator uses Penstream to calculate the required investments.

Following confirmation of each investment transaction, unit transaction details are input to Penstream and applied to individual member records. Alternatively, where STP is used the Penstream unit transaction details are prepopulated from the STP transaction confirmation.

Control activity	Auditor testing comments
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 DC Scheme unit purchase transactions, it was confirmed that unit purchases had been checked against the relevant instructions for consistency and that Penstream calculations had automatically cross-checked unit prices, fund amounts and units, with any discrepancies investigated and recorded. No exceptions noted.
2.02.2 – Unit holdings on Penstream are reconciled against the investment manager's records following each investment cycle, except where an alternative reconciliation procedure has been adopted. The file is marked accordingly by the processor and reviewer.	**2.02.2 –** For a sample of DC Scheme investment cycles, it was confirmed that unit holdings recorded on Penstream had been reconciled against the investment manager's records, or that an alternative reconciliation procedure had been applied, with evidence retained on file. No exceptions noted.

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. An eChecklist is used and progress is monitored against agreed service levels by a nominated pension administrator or the Team Leader.

Control activity	Auditor testing comments
2.03 – 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.	**2.03** – For a sample of transfer in implementations, it was confirmed that completion of each step of the process had been recorded using an eChecklist. No exceptions noted.

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 search is conducted at least annually using Penstream records to identify members reaching their NRD in the upcoming period, with each case added to Taskstream, as a retirement illustration task. Taskstream tasks are monitored by a nominated pension administrator or the Team Leader for progress and completion against agreed service standards and statutory timescale requirements.

Control activity

2.04 – Retirement illustration tasks are added to Taskstream as part of the forthcoming retirement process. 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.

Auditor testing comments

2.04 – For a sample of retirement illustration tasks, it was confirmed that retirement illustration tasks had been set up in Taskstream and that completion of each step of the process had been recorded using an eChecklist.

No exceptions noted.

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 9.01).

Control activity

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.

Auditor testing comments

2.05 – For a sample of member benefit payments, it was confirmed that Penstream calculations had been checked for reasonableness or accuracy.

No exceptions noted.

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

Process description

Authorisation for distribution of discretionary benefits is obtained by the pension administrator from the client before each payment is made, or where agreed with the client an alternative approach may be taken.

Control activity	Auditor testing comments
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, it was confirmed that appropriate authorisation had been obtained from the relevant parties. No exceptions noted.

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 3.07).

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 Cashfac Browser are generated automatically by Cashstream. The transaction authorisation process is then carried out in the Cashfac Browser. Control of user registrations and authorisation levels is detailed in another control objective (see 7.06.3).

Control activity	Auditor testing comments
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 arranged through clients' banks, it was confirmed that payment request forms had been approved by two authorised individuals and that additional client approval had been obtained where payments exceeded mandate limits. No exceptions noted.
2.07.2 – For pooled account payments below the pre-agreed limit, two authorisers approve payment transactions in the Cashfac 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 pooled account payments, it was confirmed that payment transactions had been approved by the required number of authorised individuals in the Cashfac Browser, including Gatekeeper approval where payments exceeded pre-agreed thresholds. 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 Cashfac Browser.	**2.07.3 –** For a sample of pooled account transactions exceeding pre-agreed thresholds, it was confirmed that evidence of client payment approval had been reviewed by a Gatekeeper prior to authorisation being recorded in the Cashfac Browser. No exceptions noted.

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. Payment transaction checks are covered under another control objective (see 3.07). System access controls for Bacs submission are covered under another control objective (see 7.11).

Control activity	Auditor testing comments
2.08.1 – 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.	**2.08.1** – For a sample of new pensioners, it was confirmed that transactions were independently checked for accuracy prior to posting in Penstream and that completion of each step of the process had been recorded using an eChecklist. No exceptions noted.
2.08.2 – Payroll runs for each client are reconciled for recorded changes against the previous payroll. The file is marked accordingly by the processor and reviewer.	**2.08.2 –** For a sample of payroll runs, it was confirmed that recorded changes had been reconciled against the previous payroll. No exceptions noted.
2.08.3 – 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.	**2.08.3 –** For a sample of payroll runs, it was confirmed that recorded pension entitlements had been compared against pensions in payment and that any material differences had been investigated. No exceptions noted.

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 client regarding discretionary increases. An eChecklist is used to document the calculation and processing of the indexation.

Control activity	Auditor testing comments
2.09.1 – 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.	**2.09.1** – For a sample of pension calculation output reports, it was confirmed that calculations had been spot-checked for accuracy, including the correct proportioning of indexation for members retiring within the previous year. No exceptions noted.
2.09.2 – 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.	**2.09.2 –** For a sample of pension index calculations, it was confirmed that calculated indexation totals had been appropriately recorded for payroll change reconciliation, or, where external payrolls were used, that the calculated indexation information had been provided to the responsible paying body. No exceptions noted.

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 comments
2.10.1 – 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. 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 transfer value calculations, it was confirmed that calculation outputs had been checked for reasonableness and that calculations outside agreed parameters had been referred to the Scheme Actuary or insurer for validation, with completion of the process recorded via an eChecklist. No exceptions noted.
2.10.2 – 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. 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.	**2.10.2 –** For a sample of transfer value cases prepared or validated by actuarial or insurer staff, it was confirmed that the calculation results had been appropriately authorised prior to the issue of the quotation and that completion of the process had been recorded using an eChecklist. No exceptions noted.

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 amendment 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 comments
2.11 – For processes covering the calculation of, or amendment 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.	**2.11** – For a sample of changes to Procedural Guidance and eChecklists relating to benefit calculations and transfer values, it was confirmed that changes had been reviewed for technical and structural accuracy and that reviewer approval had been recorded in the Procedural Help branch of the ticket system. No exceptions noted.

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.

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 complete except where part of a scheduled lifestyle switch. Members with online access may log in at any time to review their unit holdings.

Control activity	Auditor testing comments
2.12.1 – 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.	**2.12.1** – For a sample of investment switches, it was confirmed that Penstream calculations generating switch instructions had been checked for accuracy against the relevant switch requirements. No exceptions noted.
2.12.2 – 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.	**2.12.2 –** For a sample of investment switches, it was confirmed that completion of each step of the process had been recorded using an eChecklist. No exceptions noted.
2.12.3 – Penstream cross checks the unit price and fund amount against the number of units and any discrepancies are investigated by the pension administrator. The file is marked accordingly by the processor and reviewer.	**2.12.3 –** For a sample of investment switches, it was confirmed that Penstream had cross-checked unit prices and fund amounts against the number of units and that any discrepancies identified had been investigated. No exceptions noted.
2.12.4 – Scheduled tasks are set up on Taskstream and set to activate in advance of scheduled lifestyle switches. On completion of a lifestyle switch, the pension administrator checks the next scheduled task is in place and evidence of the check is recorded on the eChecklist.	**2.12.4 –** For a sample of lifestyle switches, it was confirmed that scheduled tasks had been set up in Taskstream in advance of the switch and that, following completion, checks had been performed to confirm that the next scheduled task was in place, with evidence recorded via an eChecklist. No exceptions noted.

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 comments
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. 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.	**3.01** – For a sample of new joiners, it was confirmed that eligibility conditions, salary caps and other relevant limitations had been reviewed, that any outstanding requirements or anomalies had been resolved, and that completion of the process had been recorded using an eChecklist. No exceptions noted.

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. Salary and other service data are used in the production of benefit statements which are distributed to active members. An eChecklist describing the data load and statement production activities, is used by the pension administrator.

Control activity	Auditor testing comments
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, it was confirmed that data had been reviewed for reasonableness and that any anomalies identified had been resolved. 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 benefit calculations, it was confirmed that Penstream calculation outputs had been checked for accuracy or reasonableness. No exceptions noted.

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/client. Data checks are performed by the pension administrator before the data is forwarded on to the Scheme Actuary/client who may conduct their own additional logic and tolerance checks.

Control activity	Auditor testing comments
3.03 – Data checks for reasonableness or accuracy are performed on extracted valuation data by the pension administration team before it is sent to the Scheme Actuary/client. The file is marked accordingly by the processor and reviewer.	**3.03** – For a sample of valuation data extracts, it was confirmed that data had been checked for accuracy or reasonableness prior to submission to the Scheme Actuary or client. No exceptions noted.

Requests to change member records are validated for authenticity

Process description

Requests to amend member records that are not submitted via Pension self-service must be authenticated by the pension administrator through identity verification or confirmation that any third-party is properly authorised, before processing, in line with data protection requirements.

Members can submit amendments to their records via Pension self-service on their Clarity from BW account (see 3.06). Access to this service requires prior registration and verification of identity (see 7.08).

Control activity	Auditor testing comments
3.04 – Before processing any changes to member records, the pension administrator verifies the member's identity or confirms that a third-party is properly authorised. Completion of this verification is recorded either on the eChecklist or, for telephone requests, in the Penstream phone note.	**3.04** – For a sample of member changes, it was confirmed that the member's identity had been verified or that appropriate third-party authorisation had been obtained prior to processing, with evidence recorded either on an eChecklist or within Penstream phone notes. No exceptions noted.

Pension Administration – 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 Pension self-service via their Clarity from BW account, 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 comments
3.05.1 – 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.	**3.05.1** – For a sample of member record modifications, it was confirmed that changes, including fast track address updates, had been independently reviewed for authority, completeness and accuracy against authorised instructions prior to processing. No exceptions noted.
3.05.2 – The fast track address update process on Penstream requires the verification of ID, or authorisation of the third-party to be confirmed, on screen before the member record can be updated, which is logically enforced by the system.	**3.05.2 –** Through observation of Penstream, confirmed that the fast track address update process on Penstream required the verification of ID and authorisation of the third-party to be confirmed, prior to the member record being updated. No exceptions noted.
3.05.3 – Bank account change notifications from members are required to be instructed in writing, except for those made by the member using Pension self-service. 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.	**3.05.3 –** For a sample of bank account change notifications, it was confirmed that changes had been supported by appropriate member instruction (or made via Pension self-service), had been independently authorised by a second pension administrator prior to posting in Penstream, and that an audit trail of changes was retained. No exceptions noted.

Requests to change member records are validated for authenticity

Process description

Members of schemes using Pension self-service via their Clarity from BW account, 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 comments
3.06.1 – Requests to change member records, submitted online via Pension 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.	**3.06.1** – For a sample of member record changes submitted via Pension self-service, it was confirmed that requests were validated by Penstream prior to posting and that changes outside valid parameters were suspended and referred for review via Taskstream. No exceptions noted.
3.06.2 – 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.	**3.06.2 –** For a sample of bank account changes submitted via Pension self-service, it was confirmed that changes were suspended in Penstream and that a Taskstream task was automatically generated for review and posting by a pension administrator or follow-up with the member where appropriate. No exceptions noted.

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, 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 Cashfac Browser are generated automatically by Cashstream.

Control activity	Auditor testing comments
3.07.1 – 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.	**3.07.1** – For a sample of payment requests, it was confirmed that payment request forms had been independently checked for completeness and accuracy prior to processing. No exceptions noted.
3.07.2 – Cashfac 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.	**3.07.2 –** For a sample of Cashfac Browser transactions, it was confirmed that transaction details generated by Cashstream had been checked for reasonableness and independently reviewed prior to processing. No exceptions noted.

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. The pension administrator cross checks all banking transactions between bank records and Cashstream for consistency and reconciles the statement against Cashstream. 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 system cross checks all banking transactions between bank records and Cashstream for consistency. The account is reconciled on a daily basis.

Control activity	Auditor testing comments
3.08.1 – 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.	**3.08.1** – For a sample of monthly treasury reconciliations, it was confirmed that Cashstream transactions had been reconciled to the accounting system following receipt of bank statements, that any differences identified had been investigated, and that a cleared balance had been achieved with reconciliation records retained. No exceptions noted.
3.08.2 – Where treasury services are provided through Barnett Waddingham's pooled account the pension administration team perform a daily reconciliation test between the bank account, Cashfac Browser segregated account records and Cashstream. Any anomalies arising are investigated and reported on the daily reconciliation report until they have been resolved. Reports confirming the reconciliations are retained.	**3.08.2 –** For a sample of daily pooled account reconciliations, it was confirmed that reconciliations had been performed between the bank account, Cashfac Browser records and Cashstream, that any anomalies identified had been investigated and resolved, and that reconciliation reports were retained. No exceptions noted.

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

Process description

All scheme and member investment or disinvestment transactions instructed by BW are initiated through a documented request or an established workflow.

The pension administrator uses Penstream either to create forms for manual completion or to generate instructions through the Straight-Through Processing (STP) system. All forms and STP-generated instructions are reviewed to ensure completeness and accuracy before the instruction is executed.

Control activity	Auditor testing comments
3.09 – All investment and disinvestment instructions generated by a pension administrator are subject to independent review by a second pension administrator. Completion of each process step is recorded on an eChecklist with both the processor and reviewer marking the file accordingly.	**3.09** – For a sample of investment and disinvestment transactions, it was confirmed that instructions had been independently reviewed by a second pension administrator and that completion of each step of the process had been recorded using an eChecklist. No exceptions noted.

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

Process description

For scheme and member investment transactions instructed by BW, the pension administrator verifies each transaction confirmation against the original instruction for accuracy. Where instructions are generated via Straight-Through Processing (STP), the system performs the verification and updates a completion status, which the pension administrator reviews. After this review, the pension administrator records transaction details in Penstream, except for STP transactions, which are pre-populated by the system. Penstream automatically validates the unit price and fund amount against the number of units, and any discrepancies are investigated.

Wholly invested unitised pooled funds maintained by BW are reconciled in Cashstream to ensure accuracy of cumulative totals.

Control activity	Auditor testing comments
3.10.1 – Upon receipt of the transaction confirmation from the investment manager, the pension administrator verifies the transaction data against the original instruction. Each step of the process is recorded on an eChecklist.	**3.10.1** – For a sample of investment transactions, it was confirmed that transaction confirmations received from investment managers had been checked against the original instructions and that completion of each step of the process had been recorded using an eChecklist. No exceptions noted.
3.10.2 – Valuation statements for wholly invested unitised pooled funds are reconciled by the pension administrator against unit holdings recorded in Cashstream and any discrepancies identified during the reconciliation are investigated and resolved. A complete reconciliation history is retained within Cashstream for audit and reference purposes.	**3.10.2 –** For a sample of wholly invested unitised pooled funds, it was confirmed that valuation statements had been reconciled against unit holdings recorded in Cashstream, that any discrepancies identified had been investigated and resolved, and that reconciliation records were retained. No exceptions noted.

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 eChecklist is used to record the completion of preparatory work on the accounts.

Control activity

3.11 – 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.

Auditor testing comments

3.11 – For a sample of schemes, it was confirmed that investment manager reports had been reviewed and relevant transactions entered into Cashstream, that balances had been reconciled to period-end investment reports, and that transactions had been recorded in the draft report and accounts prior to submission to external auditors.

No exceptions noted.

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

Process description

Prior to engagement, suppliers who will handle physical member or scheme data undergo comprehensive due diligence. This due diligence includes checks on GDPR compliance, information security, and operational resilience to confirm their capability to safeguard data and mitigate risks of theft, loss, or damage. For electronic data, this requirement is addressed under the section relating to suppliers engaged to provide IT services, which is covered by a separate control objective (see 11.01).

A formal contract, incorporating the agreed Engagement Terms, may only be signed by an authorised Partner after the supplier has successfully completed the onboarding process and demonstrated full compliance with Barnett Waddingham's requirements

Control activity	Auditor testing comments
4.01 – Each new engagement must be authorised by a Partner. Approval is evidenced by the Partner signing the engagement contract, which is retained on file.	**4.01** – Not tested – It was confirmed that no new suppliers were onboarded. Management confirmed that if there had been, the control would have operated as described.

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

Process description

Letters and statements produced by Barnett Waddingham are retained indefinitely in electronic archives on the network and in the data backup systems, except where deletion is required in line with our Data Protection and Retention policy. Access to the network and offsite backups are described under a different control objective (see 7.03, 10.01 and 10.02). 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

4.02 – Letters generated using pre-approved system standard templates are automatically approved when the pension administrator uses the system generated text. For all other letters and statements, including pre-approved system standard documents where the pension administrator has made amendments, the document is subject to review by a second pension administrator who records their approval of the letter/statement on the eFiling record.

Auditor testing comments

4.02 – For a sample of letters and statements, it was confirmed that correspondence generated using unamended pre-approved templates was automatically approved by the system, and that amended or non-standard correspondence had been independently reviewed and approved by a second pension administrator, with approval recorded on the eFiling record.

No exceptions noted.

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

Process description

Personal member information transmitted electronically is protected from unauthorised access. Unless instructed to use a client's own secure file transfer system, files are typically shared with clients and authorised third parties online using SFX (see 8.04.1). Files are typically shared with members using Pension self-service on the Clarity from BW account site. Occasionally pension administrators share files with clients, authorised third parties and members using email attachments. 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 comments
4.03.1 – Passwords must meet minimum specified complexity requirements as documented on the Password Policy, or as otherwise instructed by the client.	**4.03.1** – For a sample of system user accounts, it was confirmed that passwords met the minimum complexity requirements in accordance with the Password Policy or client-specific instructions. No exceptions noted.
4.03.2 – Breaches of email security policy which are identified by the pension administration team as a result of monitoring are brought to the attention of Team Leaders and the individual concerned, either by email or verbally.	**4.03.2 –** For a sample of identified email security breaches, it was confirmed that issues identified through monitoring had been appropriately escalated to the relevant Team Leaders and individuals concerned. No exceptions noted.

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

Process description

Any request to release information from member records that is not submitted through Pension self-service must be authenticated by the pension administrator to ensure access is limited to authorised individuals. Authentication involves verifying the requester's identity, confirming that any third-party has appropriate authorisation, or determining whether the disclosure qualifies for an exemption under data protection requirements. All such checks are subject to independent review before a written response is issued.

Pre-approved standard letter templates may be issued without review.

Verifying the identity of telephone callers is described under another control objective (see 3.04).

Control activity	Auditor testing comments
4.04 – Before disclosing member information in written communications, the pension administrator verifies the member's identity or validates that any third-party request is supported by appropriate authorisation. All outgoing communications are reviewed by a second administrator for completeness, accuracy, and compliance with data protection, and the eChecklist is marked accordingly by the processor and reviewer.	**4.04** – For a sample of written member communications, it was confirmed that the member's identity had been verified or appropriate third-party authorisation obtained prior to disclosure of information, and that outgoing communications had been independently reviewed for completeness, accuracy and data protection compliance, with completion recorded via an eChecklist. No exceptions noted.

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

Process description

When a benefit payment request is received, the member's identity must be verified to confirm eligibility and prevent payments to the wrong person. Verification is completed either by reviewing official documents (via post or secure online channels) or through a system-generated identity check before the pension administrator proceeds with payment settlement.

Control activity	Auditor testing comments
4.05 – Before any benefit payment is processed, the member's identity is verified to confirm eligibility, either through submitted ID or a system-generated check. Once verified, the pension administrator updates the eChecklist accordingly.	**4.05** – For a sample of benefit payments, it was confirmed that members' identities had been verified prior to processing, either through submitted identification or system-generated checks, and that completion of the verification had been recorded on the eChecklist. No exceptions noted.

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 pooled account arrangement. New scheme bank accounts are opened only by authorised personnel of the client.

Control activity	Auditor testing comments
4.06 – New segregated pooled account records are input on the Cashfac Browser. Before the account is activated the system requires authorisation by a Gatekeeper who checks that appropriate authorisation has been signed and received from the client.	**4.06** – For a sample of new segregated pooled account setups, it was confirmed that records had been created in the Cashfac Browser and that Gatekeeper authorisation had been obtained prior to account activation, following verification that appropriate client approval had been received. No exceptions noted.

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

4.07 – 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.

Auditor testing comments

4.07 – For a sample of offices, it was confirmed that cheque book safes/cabinets and inventories had been inspected on a quarterly basis by appointed cheque book monitors and that the results of monitoring were recorded on the relevant monitoring tasks.

No exceptions noted.

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 comments
4.08 – Combination numbers for safes and cabinets are changed every three months and distributed by local managers to authorised staff.	**4.08** – For a sample of offices, it was confirmed that safe and cabinet combination numbers were changed on a quarterly basis and that updated combinations were distributed to authorised staff. No exceptions noted.

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 reviewed 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	Auditor testing comments
4.09 – The Creator processing the Bacs payment request checks for the presence of 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.	**4.09** – For a sample of Bacs payments, it was confirmed that evidence of payment authorisation had been obtained prior to creation of the payment request, that requests had been independently reviewed and checked for accuracy before submission to Bacs, and that submission summary reports evidencing the Creator and Sender were retained on the Bacs processing system. No exceptions noted.

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 comments
4.10 – Authorisation for payment of scheme fees, invoices or levies is obtained by the pension administration team before arranging payment from scheme funds. 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.	**4.10** – For a sample of scheme fees, invoice and levy payments, it was confirmed that appropriate authorisation had been obtained prior to payment being arranged from scheme funds and that completion of the process had been recorded using an eChecklist. No exceptions noted.

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, client 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 comments
4.11.1 – 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.	**4.11.1** – For a sample of payment requests, it was confirmed that documentary evidence supporting the payment had been independently reviewed for validity prior to authorisation, and that payment requests were not authorised without evidence of this review. No exceptions noted.
4.11.2 – 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.	**4.11.2 –** For a sample of transfer payments, it was confirmed that risk-based checks had been performed and recorded using an eChecklist, and that cases requiring further investigation had been appropriately escalated to the Technical Team. No exceptions noted.

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

Process description

Existence checks are undertaken to safeguard against overpayments, for Ongoing Administration clients. The pension administrator validates pensioner existence results to ensure scheme pensioners remain eligible for benefit payments.

Where evidence of continued entitlement has not been provided, or there are indications of possible death, the pension administrator determines the appropriate next steps which may include conducting further checks, suspension of pension (see Control 7.09) or initiating the death process. (See Control 4.11.1)

Control activity	Auditor testing comments
4.12 – On receipt of the existence results, the pension administrator validates the existence status against the pensioners Penstream record. Correspondence and any actions taken where validation is not successful, are documented and retained on Taskstream.	**4.12** – For a sample of existence results, it was confirmed that existence results had been validated against pensioner records held in Penstream and that correspondence and any follow-up actions required where validation was unsuccessful had been documented and retained in Taskstream. No exceptions noted.

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. If a child fails to provide adequate evidence of educational status, further payments may be suspended.

Control activity	Auditor testing comments
4.13 – 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. Correspondence and actions are retained on the task.	**4.13** – For a sample of child pension cases subject to educational status, it was confirmed that evidence of continued entitlement had been obtained on an annual basis and that related correspondence and follow-up actions were documented and retained on the task. No exceptions noted.

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	Auditor testing comments
4.14 – 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.	**4.14** – 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.

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 comments

5.01 – For a sample of schemes, it was confirmed that scheduled monitoring tasks were in place, that contribution due dates and receipts were recorded in the contribution monitoring file, and that missing contributions were followed up with the client where applicable.

No exceptions noted.

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

5.02 – Late contributions are reported by the pension administration team 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.

Auditor testing comments

5.02 – For a sample of late contributions, confirmed that the late contributions have been reported by the pension administration team to the Partner and followed up on.

Exception noted

In one instance it was noted that a backdated pension contribution was paid late (by one day) and the breach was not reported to the Partner in a timely manner.

Management response

See management response to exception on page 28.

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 comments
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, it was confirmed that member contributions had been spot checked for reasonableness during the annual renewal, that contributions were checked against the schedule of contributions, and that any discrepancies identified had been raised with the client, with evidence of review retained. No exceptions noted.
5.03.2 – For DC schemes, exceptions generated during each contribution cycle input process are reviewed by the pension administration team and any anomalies or errors are resolved with the client. 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.	**5.03.2 –** For a sample of DC schemes, and a sample of months, it was confirmed that exceptions generated during contribution processing had been reviewed and that any anomalies or errors identified had been resolved with the client, with completion of the process recorded using an eChecklist. No exceptions noted.

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 or on Insight, our online data dashboard for clients (see 6.01).

Control activity	Auditor testing comments
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.

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

Process description

Upon discovery, transaction errors and complaints are logged and categorised by the Pension Administration team on a centralised database. Errors and complaints are managed through to resolution, under the supervision of the Quality Assurance and Governance teams, to ensure issues are monitored and resolved in line with established policy. Ongoing analysis of complaints ensures effective issue resolution and compliance.

The firmwide Complaints and Errors Policy, which is held in the Policy Handbook on Barnett Waddingham's intranet, undergoes an annual review to ensure its continued relevance, effectiveness, and alignment with current regulatory requirements.

Control activity	Auditor testing comments
5.05.1 – Transaction errors and complaints recorded in the centralised database are monitored by the Quality Assurance or Governance team upon the logging of a new issue and any actions advised or determined are recorded in the database.	**5.05.1** – For a sample of transaction errors and complaints recorded in the centralised database, it was confirmed that new issues were monitored by the Quality Assurance or Governance team and that any actions advised or determined were recorded in the database. No exceptions noted.
5.05.2 – The Governance team issues a monthly complaint analysis report to business area leaders, ensuring unresolved complaints are escalated to facilitate proactive management and timely resolution of issues.	**5.05.2 –** For a sample of monthly complaint analysis reports, it was confirmed that reports had been issued by the Governance team to business area leaders and that unresolved complaints were appropriately escalated to support proactive management and timely resolution. No exceptions noted.
5.05.3 – The firmwide Complaints and Errors Policy is reviewed by the Governance team at least annually, or earlier if significant legislative, regulatory, organisational, or technological changes arise. Evidence of review is retained within the Policy Handbook.	**5.05.3 –** Confirmed that the Complaints and Errors Policy was reviewed annually by the Governance team. Evidence of review was retained in the Policy Handbook. No exceptions noted.

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

Process description

Barnett Waddingham's Whistleblowing manual contains the operating procedure for reporting breaches to The Pensions Regulator (TPR) and sets out pension administrators' obligations regarding possible reportable breaches. The Whistleblowing manual, along with other firmwide policies and procedures, is held in the Policy Handbook on Barnett Waddingham's intranet. Employees are referred to these firmwide policies and procedures as part of their induction and through regular training arranged by the Governance Team.

Control activity

5.06 – The Whistleblowing manual is reviewed by the Governance team at least annually, or earlier if significant legislative, regulatory, organisational, or technological changes arise. Evidence of review is retained within the Policy Handbook.

Auditor testing comments

5.06 – Confirmed the Whistleblowing manual was reviewed by the Governance team on at least an annual basis. Confirmed that the evidence was retained within the Policy Handbook

No exceptions noted.

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

5.07 – 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 on a centralised register, to facilitate further review if an accumulation of incidents becomes evident.

Auditor testing comments

5.07 – For a sample of identified breaches, it was confirmed that breach reports had been reviewed by an appropriate responsible individual and that decisions regarding whether incidents should be reported, in line with the traffic-light framework, were documented, with copies retained on the centralised breaches register.

No exceptions noted.

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

Process description

The Pensions Regulator (TPR) code of practice 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

5.08 – 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. 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.

Auditor testing comments

5.08 – For a sample of notifiable event cases prepared within the Pension Administration business area, it was confirmed that reporting forms had been reviewed by an experienced pension administrator and/or the Partner prior to submission to TPR, and that completion of the process had been recorded using an eChecklist.

No exceptions noted.

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

Process description

Where Barnett Waddingham is engaged to prepare the annual Scheme Return to The Pensions Regulator (TPR), the pension administration team work with the client and their advisers to complete the return via TPR's online service. Penstream data extracts and reports are used to populate relevant sections of the Scheme Return, and to ensure data accuracy, all data entered by the pension administration team is independently reviewed. Where Barnett Waddingham is also responsible for submission, following their review of the completed return, client approval is obtained prior to filing in line with agreed timescales to ensure regulatory compliance.

Control activity

5.09 – Sections of the annual TPR Scheme Return completed by the pension administration team are reviewed for completeness and accuracy by a second pension administrator. Where Barnett Waddingham is engaged to submit the Scheme Return, client approval is obtained in advance of submission. An eChecklist is used to record the completion of each step in the process, and the file is marked accordingly by the processor and reviewer.

Auditor testing comments

5.09 – For a sample of annual TPR Scheme Return submissions, it was confirmed that sections completed by the pension administration team had been independently reviewed for completeness and accuracy, that client approval had been obtained prior to submission where Barnett Waddingham submitted the return, and that completion of the process had been recorded using an eChecklist.

No exceptions noted.

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

Process description

Where Barnett Waddingham is engaged to prepare the annual Event Report to HMRC, the pension administration team work with the client to complete the return via HMRC's online service. Outputs generated through Penstream, along with entries from Barnett Waddingham's HMRC reportable events log, which is maintained throughout the year, are used to populate relevant sections of the Event Report. To ensure data accuracy, all data entered by the pension administration team is independently reviewed. Where Barnett Waddingham is also responsible for submission, following their review of the completed report, client authorisation is obtained prior to filing in line with agreed timescales to ensure regulatory compliance.

Control activity

5.10 – The annual HMRC Event Report completed by the pension administration team is reviewed for completeness and accuracy by a second pension administrator and the file is marked accordingly. Where Barnett Waddingham is engaged to submit the Event Report, client authorisation is obtained in advance of submission.

Auditor testing comments

5.10 – For a sample of HMRC Event Reports completed by the pension administration team, confirmed review by a second pension administrator. Where Barnett Waddingham is engaged to submit the Event Report, confirmed that client authorisation was obtained in advance of submission for the majority of the sample. Confirmed that the file was marked accordingly.

Exception noted

In two instances, however, there was no explicit evidence demonstrating that client authorisation had been obtained in advance of submission of the annual HMRC Event Report.

Management response

See management response to exception on page 28.

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

Process description

Administration reports for Ongoing administration and PPF administration schemes are prepared by the pension administrator. To ensure accurate and complete reporting of administration reports within client's required timescales, reports are checked by a second member of the pension administration team prior to issue to the client.

Alternatively, clients may use Insight, our secure online dashboard, to generate real-time service level and membership movement data.

Control activity	Auditor testing comments
6.01 – Administration reports are independently reviewed by a second member of the pension administration team prior to being issued to the client and approval is noted in the task details.	**6.01** – For a sample of administration reports, it was confirmed that reports had been independently reviewed prior to issue and that evidence of approval had been recorded in the task details. No exceptions noted.

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 comments
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 benefit statements, it was confirmed that preparation, including spot checks of Penstream calculations for accuracy or reasonableness, had been reviewed by the pension administration team prior to production and that client review had taken place where requested. 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. An 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 document changes, it was confirmed that modification requests had been submitted to the Document Automation Support team where required, that changes had been implemented by the support team, and that completion of each step of the process had been recorded using an eChecklist. No exceptions noted.

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

Process description

Annual reports and accounts are prepared using a standard template, compliant with the latest Statement of Recommended Practice (SORP) for pension schemes, or as otherwise agreed with the client and their appointed auditor. Separate templates are maintained for Ongoing Administration and PPF Administration 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

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.

Auditor testing comments

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.

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 comments
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, it was confirmed that draft report and accounts reviews had been performed for completeness against SORP accounting requirements and for numerical accuracy prior to submission to the client's appointed 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 of the statutory seven-month deadline, it was confirmed that breaches had been reported to the Partner responsible for the client (or their delegate) and that consideration had been given as to whether the breach should be brought to the client's immediate attention in line with TPR whistleblowing guidance. No exceptions noted.

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

Process description

Barnett Waddingham offices are accessible using an electronic access card and/or a key. While access 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.

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

Control activity	Auditor testing comments
7.01.1 – The IT Team is notified of new employees by the People and Culture Team. Access cards for new employees are created following the onboarding process and completion of this step is recorded on the IT ticket system and subject to review.	**7.01.1** – For a sample of new joiners, it was confirmed that the IT Team had been notified by the People and Culture Team, that access cards had been created as part of the onboarding process, and that completion and review of this activity had been recorded on the IT ticket system. No exceptions noted.
7.01.2 – A log of key holders is maintained by offices where keys are used.	**7.01.2 –** For a sample of offices where keys are used, it was confirmed that a log of key holders was maintained. No exceptions noted.
7.01.3 – The IT Team are notified of staff who leave the firm by the People and Culture Team. Access cards are deactivated and retrieved following the offboarding process and completion of this step is recorded on the IT ticket system and subject to review.	**7.01.3 –** For a sample of leavers, it was confirmed that the IT Team had been notified by the People and Culture Team, that access cards had been deactivated and retrieved as part of the offboarding process, and that completion and review of this activity had been recorded on the IT ticket system. No exceptions noted.

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

Process description

All visitors must register their presence at reception. The Central Operations Team allocate a temporary electronic access 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 comments
7.02.1 – The electronic visitor log is administered by the Central Operations Team in each office.	**7.02.1** – For a sample of offices, it was confirmed that the electronic visitor log was administered by the Central Operations Team. No exceptions noted.
7.02.2 – Activation of access cards granting contractors access to specific zones is requested via the IT ticket system and approved by IT.	**7.02.2 –** For a sample of contractor access card activations, it was confirmed that requests for access to specific zones had been submitted via the IT ticket system and approved by IT prior to activation. No exceptions noted.

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 the IT Team 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 comments
7.03.1 – Access to secure rooms is restricted to IT staff and others in line with business needs.	**7.03.1** – Obtained evidence of secure room access listing, and it was confirmed that access was restricted to IT staff and other authorised individuals in accordance with business needs. 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 –** For a sample of non-network administrator access requests, it was confirmed that formal request and authorisation was obtained. This was evidenced via the IT ticket system. No exceptions noted.

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

Process description

Logical and technical access controls are implemented to restrict system and network access to authorised users and devices. This includes unique user credentials with enforced authentication standards, multi-factor authentication for externally hosted business applications, full-disk encryption on endpoint devices, and network access restrictions using certificate-based device validation.

Control activity	Auditor testing comments
7.04.1 – User access is secured through unique logon credentials and enforced password complexity standards. Multi-factor authentication (MFA) is enabled for access to externally hosted cloud-based services.	**7.04.1** – Obtained Active Directory logical access configuration, and it was confirmed that user access was secured through unique user credentials and that password complexity standards were enforced. It was also confirmed that Multi-Factor Authentication (MFA) was enabled for access to externally hosted cloud-based services. 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 –** For a sample of computers, it was confirmed that an additional encryption passcode was required to be entered before a user could log on to the device. No exceptions noted.
7.04.3 – Access to the network is restricted to authorised devices with a Network Access Control (NAC) solution in place to prevent rogue devices from connecting. Both wired and wireless network access require devices to present a valid digital security certificate before access is granted.	**7.04.3 –** Obtained network access control configuration, and it was confirmed that access to the network was restricted to authorised devices through the use of a Network Access Control (NAC) solution. It was also confirmed that both wired and wireless network access required devices to present a valid digital security certificate before access was granted. No exceptions noted.

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

Process description

IT security policies and procedures are in place to prevent unauthorised access to electronic records.

Access to networked software and electronic record keeping systems needs signing onto the network with logon and password. Access to the network is maintained by Network Administrators who normally receive instruction for users joining or leaving the business from People and Culture. In special circumstances, an IT Partner, Principal or Associate may provide alternative authorisation.

Control activity	Auditor testing comments
7.05.1 – Network access rights for new users and leavers are maintained by following either the onboarding or offboarding process and actions are recorded on the IT ticket system 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 in the IT ticket system. For a sample of leavers, it was confirmed they were disabled by following the formal leaver's process with actions recorded in the IT ticket system. **Exception noted** It was noted, however, for a few of the leavers, the disabling of access was recorded after the leaving date. It was confirmed through last login dates that none of the leaver accounts were logged into after the leaving date. **Management response** **See management response to exception on page 29.**
7.05.2 – Periodic integrity checks are performed on user accounts and any actions taken on exceptions are documented.	**7.05.2 –** For a sample of user accounts, it was confirmed that periodic integrity checks had been performed and that any actions taken in relation to identified exceptions were documented. No exceptions noted.

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 comments
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** – Obtained evidence of the Bacs processing system access configuration, and it was confirmed that additional password, user privilege and access controls were in place, including the use of Bacs smartcard technology, and that access was allocated and maintained by authorised Bacs System Administrators. 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 –** Obtained evidence of STP access configurations, and it was confirmed that additional password, user privilege and access controls were in place and allocated and maintained by authorised STP System Administrators, and that further access restrictions using IP and certificate controls were enforced and maintained by Network Administrators. No exceptions noted.
7.06.3 – The Cashfac Browser has additional password, user privilege and access controls which are maintained by authorised users and Gatekeepers.	**7.06.3 –** Obtained evidence of the Cashfac Browser access configuration, and it was confirmed that additional password, user privilege and access controls were in place and were maintained by authorised users and Gatekeepers. No exceptions noted.

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 comments
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** – Obtained evidence of endpoint security configuration, and it was confirmed that password protected screen savers were enabled on servers, desktop PCs and laptop computers and activated after a defined period of inactivity. No exceptions noted.
7.07.2 – A log of users' policy acknowledgements is retained. The People and Culture team identify and resolve overdue policy acknowledgements.	**7.07.2 –** For a sample of staff, it was confirmed that a log of users' policy acknowledgements was maintained and that overdue policy acknowledgements were identified and resolved by the People and Culture team. No exceptions noted.

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 8.04).

Control activity	Auditor testing comments
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** – Obtained the network access configuration settings, and it was confirmed that a two-step login process and that lock out controls were in place following successive failed login attempts. No exceptions noted
7.08.2 – Standard procedure is followed to grant members access to their records.	**7.08.2 –** For a sample of member access requests, it was confirmed that standard procedure had been followed to grant members access to their records. No exceptions noted.
7.08.3 – The Clarity from BW account site 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 or Governance Committee and noted in meeting minutes.	**7.08.3 –** For a sample of annual penetration testing activities, it was confirmed that penetration testing of the Clarity from BW account site had been performed, that test results were reviewed and actions identified and logged where required, and that reports were reviewed by the IT or Governance Committee with evidence noted in meeting minutes. No exceptions noted.

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 4.09 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 pension administrator and input to the system. The inputs are reviewed for accuracy by another pension administrator who then applies the change to the system.

Auditor testing comments

7.09 – For a sample of changes to bank account details, additions of new members to payrolls, and suspension or unsuspension of payments, it was confirmed that inputs prepared by a pension administrator had been independently reviewed for accuracy and applied to the system by a second pension administrator.

No exceptions noted.

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 comments
7.10 – Permissions for different users are authorised, allocated and maintained by group managers in UaG.	**7.10** – Obtained evidence of the UaG access group configuration, and it was confirmed that only Penstream Security Users can access and amend user access permissions. No exceptions noted.

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 comments
7.11.1 – Access to the Bacs processing system software is controlled by the IT Team. Any changes are recorded in the IT ticket system.	**7.11.1** – For a sample of access changes to the Bacs processing system, it was confirmed that access was controlled by the IT Team and that changes had been 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 –** Obtained evidence of the Bacs system access configuration, and it was confirmed that Creators and Senders required a Bacs smartcard and associated PIN, that smartcard allocation was controlled, and that system access enforced segregation of duties such that users could either create or authorise Bacs submissions, but not both. No exceptions noted.

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 comments
7.12 – The ability to add or remove users from the editing group is restricted by system permission settings to authorised users.	**7.12** – Obtained evidence of the system permission configuration, and it was confirmed that the ability to add or remove users from the editing group was restricted to authorised users. No exceptions noted.

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. 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.

Control activity	Auditor testing comments
8.01.1 – 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.	**8.01.1** – Obtained evidence of the system access configuration, and it was confirmed that the ability to release submission files was restricted to authorised staff and that access restrictions were logically enforced by the system and maintained by group managers within UaG. No exceptions noted.
8.01.2 – 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.	**8.01.2 –** Obtained submission files logs confirming release to HMRC Online Services. For a sample of failures, obtained evidence that submission completion was monitored with any failures reported to the relevant team through to remediation. No exceptions noted.
8.01.3 – An investigation and resolution of communication failures between the BW GovTalk Submitter and HMRC Online Services are recorded in the IT ticket system.	**8.01.3 –** For a sample of communication failures between the BW GovTalk Submitter and HMRC Online Services, it was confirmed that investigations and resolutions had been recorded in the IT ticket system. 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 comments
8.02.1 – 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.	**8.02.1** – For a sample of communication failures with the DPS system, it was confirmed that automated error reports had been generated by the system and submitted to the IT ticket system for investigation and resolution. No exceptions noted.
8.02.2 – Notices that could not be processed automatically are reported for manual adjustment as required. As part of the regular payroll process, the pension administrator checks for unprocessed notices and records the check on the Payroll run eChecklist.	**8.02.2 –** For a sample of payroll runs, it was confirmed that notices which could not be processed automatically had been identified for manual adjustment and that checks for unprocessed notices had been performed and recorded on the payroll run eChecklist. No exceptions noted.

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 comments
8.03 – The server processes managing communications with the DPS and HMRC Online Services are continuously checked by network monitoring software. Errors are reported automatically via the IT ticket system. Remediation actions taken by the IT Team are recorded on the IT ticket system.	**8.03** – Obtained evidence of network monitoring and incident management configuration and together with observation, it was confirmed that server processes managing communications with the DPS and HMRC Online Services were continuously monitored by network monitoring software, that errors were automatically reported via the IT ticket system, and that remediation actions taken by the IT Team were recorded on the IT ticket system. No exceptions noted.

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 4.03.1), services available via Clarity from BW accounts or API services.

Online functionality within Pension 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 comments
8.04.1 – All transmissions of data through the online services available via the Clarity from BW account site are sent using HTTPS secure channels. Only TLS 1.2 or higher are supported.	**8.04.1** – Obtained evidence of system configuration, and it was confirmed that all data transmissions through the online services available via the Clarity from BW account site were sent using HTTPS secure channels and that only TLS version 1.2 or higher was supported. No exceptions noted.
8.04.2 – All transmissions of data to the third-party print and mailing service are sent using HTTPS secure channels.	**8.04.2 –** Obtained evidence of system configuration, and it was confirmed that all transmissions of data to the third-party print and mailing service were restricted to using HTTPS secure channels. 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 comments
8.05 – Electronic data transmissions are made over the internet using HTTPS secure channels.	**8.05** – Obtained evidence of system configuration, and it was confirmed that electronic data transmissions over the internet were restricted to HTTPS secure channels. 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 comments
8.06.1 – Electronic data transmissions are made over the internet using HTTPS secure channels.	**8.06.1** – Obtained evidence of system configuration, and it was confirmed that electronic data transmissions were restricted to using HTTPS secure channels over the internet. No exceptions noted.
8.06.2 – 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.	**8.06.2 –** Obtained evidence of the DPS data retrieval logs, and it was confirmed that unique incremental data block IDs were recorded during each retrieval exercise and that the highest ID was used as the starting point for the subsequent retrieval to ensure completeness of new records. No exceptions noted.

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 comments
8.07.1 – Incoming emails are scanned to identify potential threats by the service provider and Barnett Waddingham's email security gateway. In addition, an advanced AI based analysis tool is utilised to further scan all incoming emails for advanced threats including email compromise and take-over. Files opened via email are subject to on-access scanning to identify potential threats. Quarterly health checks are performed by the IT Team to review policies and parameters and any recommendations for change are detailed on monthly reports to IT Committee.	**8.07.1** – Obtained evidence of email security and monitoring configurations, and it was confirmed that incoming emails were scanned for potential threats by the service provider and Barnett Waddingham's email security gateway, supported by advanced AI-based analysis for detection of sophisticated threats, and that files opened via email were subject to on-access scanning. It was also confirmed for a sample of quarters that health checks were performed by the IT Team to review policies and parameters, with any recommendations for change documented within reports provided to the IT Committee. No exceptions noted.
8.07.2 – Emails containing known viruses are logged, blocked and deleted by the email service provider. FTP servers are protected by enhanced endpoint detection and response (EDR) controls to monitor, detect, and respond to suspicious activity.	**8.07.2 –** Obtained evidence of email and server security configurations, and it was confirmed that emails containing known viruses were logged, blocked and deleted by the email service provider, and that FTP servers were protected by enhanced endpoint detection and response (EDR) controls to monitor, detect and respond to suspicious activity. No exceptions noted.
8.07.3 – Files received through Pension self-service and SFX via the Clarity from BW account site are virus scanned during the transmission process to identify potential threats.	**8.07.3 –** Obtained evidence of file transfer and security configurations, and it was confirmed that files received through Pension self-service and SFX via the Clarity from BW account site were virus scanned during transmission to identify potential threats. No exceptions noted.

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 comments
8.08 – Access privileges require authorisation through the IT ticket system by an IT Partner, Principal, Associate or Team Leader and are created on a temporary basis.	**8.08** – For a sample of access privilege requests, it was confirmed that access had been authorised through the IT ticket system by an appropriate IT Partner, Principal, Associate or Team Leader and that access was granted on a temporary basis. No exceptions noted.

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

8.09 – Virus protection definitions are kept up to date through Windows Server Update Services (WSUS) and EDR prevention policies. Email alerts are triggered in the event a virus is found. Notifications are sent to our IT Security Team for review and necessary action is taken. Machines are isolated from the network if necessary.

Auditor testing comments

8.09 – Obtained evidence of the antivirus update settings, and it was confirmed that virus protection definitions were kept up to date that, alerts were triggered when viruses were detected, and that email alerts were sent to the IT Security Team for review and appropriate action, including isolation of affected machines where required.

No exceptions noted.

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 penetration experts. Multiple service providers are used in order to obtain expanded test coverage on a rotational basis.

Control activity	Auditor testing comments
8.10 – The network penetration testing reports are reviewed by the IT Security Team and the IT Committee and any actions required are noted in meeting minutes. All risk items identified are logged on the IT ticket system and remediation actions taken by the IT Team are recorded on the IT ticket system.	**8.10** – For a sample of network penetration testing reports, it was confirmed that reports had been reviewed by the IT Security Team and the IT Committee, that actions required were noted in meeting minutes, and that identified risk items and remediation actions had been logged and tracked through the IT ticket system. No exceptions noted.

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 comments
8.11.1 – Modifications to firewall configuration settings are subject to a change management process and must be authorised by the IT Change Approval Board (CAB) before implementation.	**8.11.1** – For a sample of firewall changes, confirmed that modifications to firewall configuration settings were subject to a formal change management process and required authorisation by the IT Change Approval Board prior to implementation. No exceptions noted.
8.11.2 – Changes to web access can only be made by Network Administrators and require authorisation by the IT Change Approval Board (CAB) before implementation.	**8.11.2 –** Obtained evidence of web user access permissions, and it was confirmed that changes to web access could only be made by Network Administrators and that for a sample of changes, authorisation by the IT Change Approval Board was obtained prior to implementation. No exceptions noted.

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

Process description

Perimeter and internal segmentation firewalls are installed and changes are tested and approved by a list of suitable approvers.

Control activity	Auditor testing comments
8.12 – Perimeter and internal segmentation firewall reviews are conducted by the IT Operations Team and any identified shortcomings are rectified. Records evidencing action taken are retained within IT Change Approval Board (CAB) tickets.	**8.12** – For a sample of firewall reviews, it was confirmed that perimeter and internal segmentation firewall reviews had been conducted by the IT Operations Team, that identified shortcomings had been remediated, and that evidence of actions taken was retained within Change Approval Board (CAB) tickets. No exceptions noted.

Development and implementation of both inhouse 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.

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

Control activity	Auditor testing comments
9.01.1 – Penstream development activity, including work specification and testing of changes, is approved by the Software Feature Owner and evidence of approval is retained on the eChecklist.	**9.01.1** – For a sample of Penstream development activities, it was confirmed that work specifications and testing of changes had been approved by the Software Feature Owner and that evidence of approval was retained on the ticket. No exceptions noted.
9.01.2 – Changes to Penstream are developed and tested independently of the live system. The development environment is contained on a separate network.	**9.01.2 –** For a sample of Penstream changes, it was confirmed that changes were developed and tested independently of the live system and that the development environment was hosted on a separate network. No exceptions noted.
9.01.3 – A standard release procedure is followed for new code to go live. The Business Signoff is recorded on an eChecklist.	**9.01.3 –** For a sample of Penstream changes, it was confirmed that changes had been developed and tested independently of the live system, that a standard release procedure had been followed for deployment, and that Business Sign-off had been obtained with evidence recorded on an eChecklist. No exceptions noted.
9.01.4 – All changes to Penstream source code are recorded through an Azure DevOps Git pull request. All activity is recorded in Azure DevOps and enforces code review by a second developer prior to addition to the development branch.	**9.01.4 –** For a sample of Penstream source code changes, it was confirmed that changes had been recorded through Azure DevOps Git pull requests and that code reviews by a second developer were enforced prior to changes being merged into the development branch. 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 comments
9.02.1 – 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 from the IT Change Approval Board or an IT Partner, Principal or Associate. Testing and approval records are maintained.	**9.02.1** – For a sample of non-Penstream development activities and database changes, it was confirmed that requirements had been allocated to developers by IT Team Leaders, that new software and upgrades were tested prior to release, and that appropriate authorisation had been obtained from the IT Change Approval Board or an IT Partner, Principal or Associate, with testing and approval records retained. No exceptions noted.
9.02.2 – Changes to network infrastructure require authorisation from the IT Change Approval Board or by an IT Partner, Principal or Associate. Affected services are identified and recorded together with details of any testing checks and authorisation.	**9.02.2 –** For a sample of network infrastructure changes, it was confirmed that changes had been appropriately authorised by the IT Change Approval Board or an IT Partner, Principal or Associate, and that affected services, testing performed and authorisation details had been identified and recorded. No exceptions noted.

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

Process description

For system maintenance or development activities requiring migration or modification of client data an audit trail is retained for any such change activity. Actions are authorised and checked by staff appropriate to the nature of the change.

Control activity	Auditor testing comments
9.03 – 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.	**9.03** – For a sample of system maintenance and development activities involving client data, it was confirmed that changes had been performed by authorised IT or specialist Pension Administration staff and that details of the changes, together with evidence of authorisation and any testing or verification activities, had been recorded on the IT ticket system or Taskstream. No exceptions noted.

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 change process. Changes are recorded.

Control activity	Auditor testing comments
9.04 – Changes to systems require authorisation from the IT Change Approval Board or by an IT Partner, Principal or Associate. Affected services are identified and recorded together with details of any testing checks and authorisation.	**9.04** – For a sample of system changes, it was confirmed that changes had been authorised by the IT Change Approval Board or an IT Partner, Principal or Associate, and that affected services, testing performed and authorisation details had been identified and recorded. No exceptions noted.

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 comments
10.01.1 – Fire extinguishers are maintained in compliance with fire safety regulations. All offices are equipped with P50 units which have reduced maintenance requirements and do not require annual servicing. A competent person performs a monthly visual check of each unit and a six-monthly inspection of the magnetic gauge. Records of these inspections are retained.	**10.01.1** – For a sample of offices, it was confirmed that P50 fire extinguishers were maintained in compliance with fire safety requirements, that monthly visual checks and six-monthly magnetic gauge inspections were performed by a competent person, and that records of these inspections were retained. No exceptions noted.
10.01.2 – 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.	**10.01.2 –** For a sample of UPS devices, it was confirmed that devices were network-connected to report status and power events. In addition, evidence of alerting configuration was obtained, and it was confirmed that Network Administrators were automatically notified of critical UPS functionality incidents via email alerts and/or audible and visual alarms. No exceptions noted.
10.01.3 – Temperature and moisture readings outside specified thresholds as well as any detected water ingress are monitored by Network Administrators.	**10.01.3 –** For a sample of offices, confirmed that temperature and moisture thresholds have been configured as well as water ingress monitoring. No exceptions noted.
10.01.4 – 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.	**10.01.4 –** For a sample of secure room inspections, it was confirmed that Network Administrators had performed periodic checks for unexpected audio activity and that completion of these checks had been recorded within the IT ticket system. No exceptions noted.

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 comments
10.02.1 – Backup service reports are reviewed daily and results are kept on record.	**10.02.1** – For a sample of days, it was confirmed that backup service reports were reviewed and that the results of the reviews were retained. No exceptions noted.
10.02.2 – 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.	**10.02.2 –** For a sample of months, it was confirmed that integrity checks of third-party server backups had been performed through restoration of sample data, that the results of these tests had been documented, and that any failures identified were appropriately investigated. No exceptions noted.
10.02.3 – Backups are retained on third-party servers for at least thirty days.	**10.02.3 –** Obtained evidence of the backup retention schedule, and it was confirmed that backups were retained on third-party servers for a minimum of thirty days. No exceptions noted.
10.02.4 – Each year a full backup snapshot is taken and stored by the service provider, segregated from all other existing backups.	**10.02.4 –** It was confirmed that a full backup snapshot had been taken in the year and stored by the service provider, segregated from all other existing backups. 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 comments
10.03.1 – 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.	**10.03.1** – Obtained the configurations settings of the performance and capacity system and it was confirmed that networked devices were monitored on an ongoing basis and that any issues identified were remediated by Network Administrators. No exceptions noted.
10.03.2 – 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.	**10.03.2 –** Obtained evidence of email monitoring and alerting configuration, and it was confirmed that email efficiency was monitored using queue length metrics and that if the length is exceeded automated alerts are triggered. No exceptions noted.

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

10.04 – 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 comments

10.04 – Obtained the annual disaster recovery simulation report, and it was confirmed the test was completed within the audit period and that outcomes were documented and reviewed by the IT Committee.

No exceptions noted.

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

Process description

The Accountable Executive for Continuity (AEC) and Responsible Person for Continuity (RPC) are 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. They are responsible for maintaining and updating the plan and for ensuring, in conjunction with the IT Operations and IT Security teams, that all relevant testing takes place.

Control activity

10.05 – The business continuity plan is reviewed and tested at least annually. The AEC and RPC reports the results of all tests to the Operational Resilience Steering Committee & PRCC and will track and report on any recommendations or actions resulting from the tests.

Auditor testing comments

10.05 – Obtained the business continuity plan, testing and meeting minutes and it was confirmed the plan was reviewed and tested within the audit period and the results were reported to the PRCC.

No exceptions noted.

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. 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.

Control activity	Auditor testing comments
10.06 – Service Desk Overview reports, which include performance statistics, are prepared each month by IT Team Leaders for the Head of IT to consider and discuss with IT Committee if appropriate.	**10.06** – For a sample of months, obtained the IT Service Desk Overview report, and it was confirmed the Ticket monitoring was reported to the Head of IT and IT Committee. No exceptions noted.

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-party suppliers. Contracts with suppliers are agreed only once the supplier has successfully completed the supplier onboarding process and is able to fully meet Barnett Waddingham's requirements from a legal, regulatory, environmental, sustainability and Cyber Security perspective. The decision to appoint the supplier is made by a Partner and if appointed, the relationship is overseen by a Partner.

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

Control activity	Auditor testing comments
11.01.1 – 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. Only Partners are authorised to sign contracts on behalf of Barnett Waddingham.	**11.01.1** – For a sample of contracts for new suppliers engaged to provide IT services and/or products it was confirmed a Partner reviewed and signed the contract on behalf of Barnett Waddingham. No exceptions noted.
11.01.2 – A Partner, Principal or Associate will perform or oversee a review of each supplier at a frequency linked to the level of risk associated with the supplier. Action points arising from the meetings with suppliers who provide IT services and / or products are agreed with the Head of IT and any high impact or potentially disruptive issues arising are discussed at IT Committee meetings.	**11.01.2 –** For a sample of providers, it was confirmed that Partner oversight of the service, including any actions arising as needed, was performed. No exceptions noted.

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 supplier ensures regular monitoring of the outsourced service.

Control activity	Auditor testing comments
11.02 – Regular service reports are submitted by the network service provider against pre agreed service level objectives. Reports are reviewed by the Head of IT and any issues arising are discussed at IT Committee meetings.	**11.02** – For a sample of IT Committee meetings, it was confirmed that service provider reports were reviewed and discussed. No exceptions noted.

Glossary

AAF	Audit and Assurance Faculty (of the Institute of Chartered Accountants in England and Wales).
API (Application Programming Interface)	Used to enable data exchange between systems such as Penstream and third-party services.
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.
Bacs / Bacs Bureau	An electronic system used for processing batches of payment instructions in the UK.
Benefit Specification	A document outlining how scheme rules are interpreted and applied within administration systems for a specific client.
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.
Cashfac Browser	Software application from Cashfac PLC providing banking platform.
Clarity from BW	Barnett Waddingham's online registration portal for clients and members that brings together a wide range of services from across Barnett Waddingham."
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.
Complementary Subservice Organisation Controls (CSOCs)	Subservice Organisation Control Activities which complement Service Organisation Control Activities.
Contribution Monitoring File	Record used to track expected and received pension contributions and identify late or missing payments.
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.
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.
EDR (Endpoint Detection and Response)	Cybersecurity technology used to detect and respond to threats on endpoint devices.
eFiling	An electronic data management and document imaging system that integrates with Penstream, Taskstream and Pension self-service, allowing scanned documents to be displayed directly alongside a member's internal Penstream record.
Gatekeeper	A pooled banking permissions group for authorising transactions, comprising Pension Administration Partners and Principals.
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.
Insight	An online dashboard for trustees, designed to make pension scheme analytics available to our clients, presented in a clear way that allows instant analysis.
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).
IT	Information Technology.
IT Change Approval Board	Provides a secondary context sensitive approval to existing application and component level approvals for change and release into BW's production environments.
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.
MFA (Multi-Factor Authentication)	A security process requiring more than one method of authentication (e.g. password plus device verification).
NAC (Network Access Control)	Security approach controlling access to a network based on device identity and compliance.

Network Administrator	Network operations and IT support team staff with elevated network domain access privileges to maintain Barnett Waddingham's IT infrastructure and network.
Normal Retirement Date (NRD)	The age or date specified in scheme rules at which a member is entitled to take retirement benefits without reduction.
Operational Resilience Steering Committee	Coordinates and guides the development and implementation of operational resilience improvement actions across Barnett Waddingham.
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 self-service	A BW online platform which allows scheme members to confidentially manage key aspects of their pension arrangements.
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.
Project manager	An individual responsible for managing a project, ensuring it is delivered on time, within scope, and to the required quality, such as onboarding a new client.

Project Planning Lead	System architect (senior IT software programmer).
RAID Log	Risk, Action, Issue and Decision log used to track and manage project risks, actions, issues, and key decisions during client onboarding.
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.
Software Feature Owner	Responsible for the lifecycle of an individual software feature.
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.
Subservice Organisation	A Service Organisation used by the Service Organisation.
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 system used across the organisation to log, track and resolve IT and other support-related issues and service requests.
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	Client using our pension administration services.

Appendix A – Statement by the Service Auditor

The Service Auditor's Report, as set out at pages 127 to 129, has been prepared solely in accordance with terms of engagement agreed by the Pension Administration 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 of reporting on the Control Activities in providing an independent conclusion on the Management Statement set out at page 23 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

Our Ref: JT/AAF01/20/2025.26

RSM

Strictly Private & Confidential
REASONABLE ASSURANCE REPORT

RSM UK Risk Assurance Services LLP
25 Farringdon Street
London
EC4A 4AB
United Kingdom
T +44 (0)20 3201 8000
rsmuk.com

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

27 May 2026

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 Partners (the 'Partners') 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 3 November 2025.

SCOPE

We have been engaged to report on Barnett Waddingham LLP's description of its pension administration services and related information technology throughout the period 1 April 2025 to 31 March 2026 (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 third-party Service Organisations (the 'Subservice Organisation'). 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 Subservice Organisations. Our examination did not extend to Control Activities of these Subservice Organisations.

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.

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.

RSM

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 22, 24 to 121 and the accompanying Partners Statement set out on page 23, including the completeness, accuracy, and method of presentation of the Description and the Partners 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 page 24 and 25, include the internal Control Objectives developed for pension administration and related information technology as set out in the Technical Release AAF 01/20 ('AAF 01/20'), issued by the Institute of Chartered Accountants in England and Wales (ICAEW) and the International Standard on Assurance Engagements 3402 ('ISAE 3402'), issued by the International Auditing and Assurance Standards Board except where stated otherwise.

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), International Standards on Assurance Engagements 3402, and AAF 01/20 issued by the ICAEW. 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 page 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 controls. Our procedures included assessing the risks that the Description is not fairly presented and that the Control Activities were not suitably designed or operating effectively to achieve the related Control Objectives stated in the Description.

RSM

Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related Control Objectives stated in the Description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the description and the suitability of the Control Objectives stated therein.

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

OUR INDEPENDENCE AND QUALITY CONTROL

RSM UK Risk Assurance Services LLP applies International Standard on Quality Management (UK) 1 'Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or other Assurance or Related Services Engagements' (ISQM (UK) 1), which requires RSM UK Risk Assurance Services LLP to design, implement and operate a system of quality management including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

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 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.

OPINION

In our opinion, in all material respects, based on the Criteria described in the Service Organisations Partner's Statement on page 23:

a) the Description on pages 3 to 22, 24 to 121 fairly presents the Service Organisation's pension administration activities and related information technology as designed and implemented throughout the period from 1 April 2025 to 31 March 2026;

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 2025 to 31 March 2026;

c) the Control Activities tested, which together with the Complimentary User Entity Controls referred to in the scope paragraph of this assurance report, 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 2025 to 31 March 2026.

DESCRIPTION OF TESTS OF CONTROLS

The specific controls tested and the nature, timing and results of those tests are detailed on pages 30 to 121.

RSM UK Risk Assurance Services LLP

RSM UK Risk Assurance Services LLP

London, 27 May 2026

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/AAF01/20/2025.26
3 November 2025

Strictly Private & Confidential

The Partners
Barnett Waddingham LLP
2 London Wall Place
123 London Wall
London
United Kingdom
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 October 2024.

RESPONSIBILITIES OF THE 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.

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. An illustration of the form of our report is attached as Appendix 1.

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 the 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 together with the ethical requirements in the International Ethics Standards Board for Accountants' International Code of Ethics for Professional Accountants (including International Independence Standards) (the 'IESBA Code'). As has been agreed with the Entity, for the purposes of this engagement we will comply with the independence requirements applicable to assurance engagements in the IESBA Code / Revised Ethical Standards issued by the Financial Reporting Council / ICAEW Code of Ethics as if they applied to the Service.

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 Service Auditor's Report will be issued on the basis that it must not be recited or referred to or disclosed, in whole or in part, in any other document or to any other party, without the express prior written permission of the Service Auditor. We permit the disclosure of the Service Auditor's Report, in full only, to existing 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 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 website.

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 existing 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 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 Partners 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.'

RSM

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 October 2024

Contents noted and agreed for and on behalf of Barnett Waddingham

Paul Latimer

Signature

Partner, Barnett Waddingham LLP

Job Title

04/11/25

Date

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