HYMANS ROBERTSON

AAF 01/20 and ISAE 3402 Assurance Report

Internal Controls for Pensions Administration Services

Report for the Period 1 February 2022 to 31 January 2023

Contents

1	Introduction	1
2	Background and Organisation Structure	2
3	Pensions Administration Business Unit	5
4	The Protection of Client Data	8
5	Report from the Partners of Hymans Robertson LLP	15
6	Service Auditor Statement	21
7	Service Auditor Report	22
8	Summary of Control of Objectives	25
9	Control Objectives and Control Activities	27
10	Club Vita - Information Security	76
Appendix		

1 Introduction

The Partners of Hymans Robertson LLP ("Hymans Robertson") are pleased to present our report detailing the control procedures that are in place relating to Hymans Robertson's business operations in providing pension administration and pension database services.

This report covers the year ended 31 January 2023 and has been prepared in accordance with the Technical Release AAF 01/20 "Assurance Reports on Internal Controls of Service Organisations made available to Third Parties" published by the Institute of Chartered Accountants in England and Wales ("the ICAEW") and the International Standards on Assurance Engagements 3402 (ISAE 3402). This report provides information and assurance to our clients and their external auditors on the design and description of the operational controls within our pensions administration business unit.

Hymans Robertson is a limited liability partnership that has been providing pension administration services since 1984.

We provide a full range of pension administration services, including:

- Pension Administration
- Pensioner Payroll
- Treasury and Cash Management
- Pension Plan Accounting and Financial Statement Preparation and
- Administrative Consultancy Support
- Data Journey Projects.

We operate in partnership with our clients and their other advisors, to deliver a client driven, bespoke, high quality and accurate administration service using a combination of excellent staff and market leading systems. As a business, we adopt tight internal controls and compliance to ensure we supply our clients with accurate advice and information, and embedded within our culture is a comprehensive and well-structured approach to risk management.

At Hymans Robertson we are constantly striving to find ways to improve the delivery of service to our clients. The Partners of Hymans Robertson, therefore, welcome the opportunity to have our administration procedures reviewed by external auditors. Hymans Robertson has appointed RSM UK Risk Assurance Services LLP, independent service auditors, to appraise the design and description of the controls within our administration business unit. Due to the change in service auditors, we have also taken the opportunity to perform a rigorous review of the controls in place, rewording and updating them as appropriate. The Service Auditor report is set out in Section 7.

Effective pension scheme management is a pension scheme's trustees' responsibility. This report provides our clients, prospective clients and Trustees with information and assurances about our processes and the strongly controlled environment that is in place to assist us in continuing to deliver high quality, pension administration services to our increasing range of schemes.

2 Background and Organisation Structure

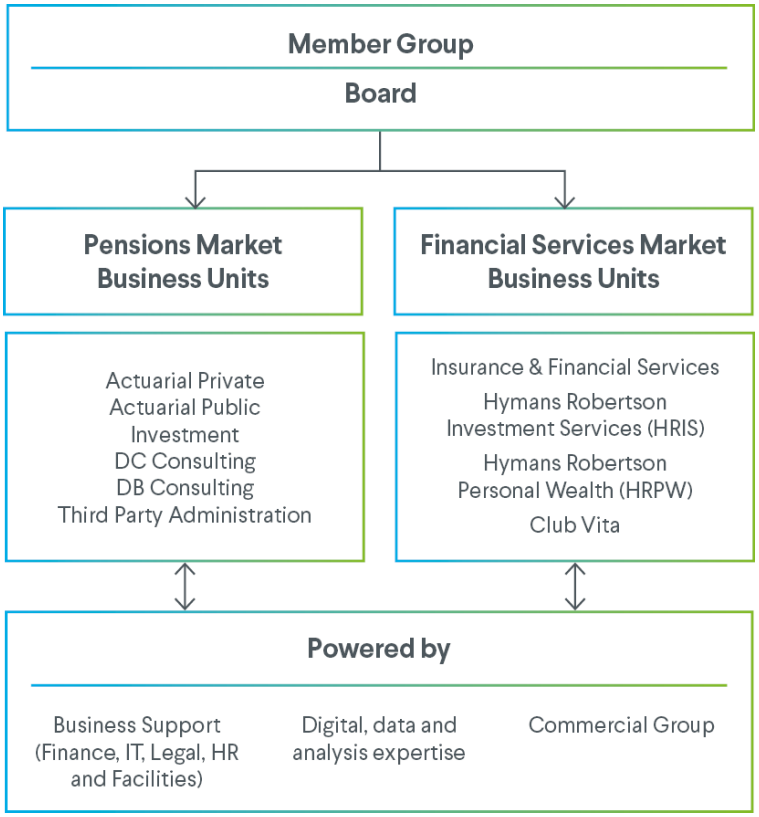
Founded in 1921, we are one of the longest established independent firms of consultants and actuaries in the UK. We are a limited liability partnership; ownership lies with the Partners who are fully involved in the day-to-day management of Hymans Robertson.

Specialising in advisory and management services to the occupational pensions market, in both private and public sectors, we provide all the core services such as:

- Actuarial consultancy
- Investment consultancy
- Pension scheme design and management
- Third party administration
- Corporate pension consulting and
- Flexible benefits broking and consulting.

We also offer independent advice to financial services institutions, as well as data and technology solutions.

This rich mix of services enables us to meet the entire pension and benefits needs of our clients. We employ over 1,100 people within our four offices in London, Glasgow, Birmingham and Edinburgh and the chart below outlines our structure:



Our Member Group and Partner Board set the strategic course for Hymans Robertson and oversee our six pensions market business units and three financial services market business units. All business units are supported by the functions shown in the 'powered by' box at the bottom of the chart.

Club Vita

Club Vita LLP ("Club Vita") is a company 100% dedicated to helping companies and pension schemes manage longevity risk. Club Vita's principal activity is the provision of services based on the performance of research and analysis into the longevity of participants in pension schemes. The analysis is based on the pooled data records of over 250 pension schemes of employers representing a wide range of industries.

Club Vita is a wholly owned subsidiary of Hymans Robertson. The operations are governed separately to other operations within Hymans Robertson but are operated exclusively within Hymans Robertson premises using Hymans Robertson resources. The company was established in 2008 and adopted many of the underlying foundation services that have been successfully deployed for many years within Hymans Robertson's Third-Party Administration operations.

The effective application of robust operational controls is important to Club Vita's clients and hence the Club Vita business. Club Vita needs to be able to demonstrate to its clients that the operational controls are fit for purpose. In addition to internal audits and reviews Club Vita considers the external AAF audit will help it to demonstrate the suitability of the operational controls to its clients. Our report demonstrates the additional controls restricting access to systems and data applicable to Club Vita.

International Partner

We are the exclusive UK pensions partner with Abelica Global, the international organisation of independent actuarial firms. Our partnership with Abelica Global enables us to provide benefits to our global clients without compromising our independent status.

Feedback and Performance

Feedback from our clients is vital, and we regularly assess satisfaction levels through our Voice of Client survey. With 98% of our clients willing to recommend us to a colleague, our clients are pleased with our relationships. This attributes to the fact that we always tailor our advice to meet clients' needs.

The high standard of our services has been recognised at many industry awards, including the Workplace Savings and Benefits Awards and Insurance Asset Risk Awards, where we won Pension Consultant of the year 2022 and Investment Strategy Consultant of the year 2021, respectively. We have recently been named DC Consultancy of the Year and Risk Reduction Advisor of the Year at the Professional Pensions Awards 2023. We were also named as one of the top 10 flexible employers at the Flexibility Works Employer Awards.

The Pensions Administration Standards Association (PASA) was established to promote and improve the quality of pension administration services for UK pensions schemes. Both The Pensions Regulator (TPR) and the Department for Work and Pensions (DWP) identify that good administration can be demonstrated by independent accreditation. In 2015, our administration practice became only the fourth administrator (and second Third-Party Administrator) to be accredited by PASA for the quality of our administration service. Attaining and retaining PASA accreditation is the gold standard for high-quality pension administration.

Finally, we are also a Living Wage employer, illustrating how we truly value our employees - a team that we are immensely proud of!

We maintain a significant presence in the industry through speaking at events, responding to government and regulatory consultations, issuing press releases, sharing our insights, and thought leadership and through our representation on various industry and professional committees. It is part of our culture for

consultants to understand and be involved in the development of the bigger picture for pensions. This enables our clients to benefit from insightful advice and to be on the front foot with any change.

Our Guiding Values

Our purpose – together, building better futures – is at the heart of the firm, and why we exist. It's about the value we create for society and how we make a positive impact within and beyond our firm. We believe all businesses have a responsibility to use their influence to make a positive impact in the world around them. For their people, their clients and customers, the communities they work in, and ultimately, in the world we all live in. We take responsibility seriously and consider it a privilege.

We have recently been accredited as a **B Corp** business, having been assessed in how we manage our environment, our community at large, our staff, our governance and our clients and customers. We are delighted to have achieved this status and it is a positive affirmation of our credentials as a purpose led firm and our belief that our business is a force for good.

Through initiatives such as our charity, the **Hymans Foundation**, together with our volunteering initiative, **Helping Hands**, as well as the myriad of other, local, community initiatives we participate in each year, we are proud of our corporate social responsibility.

We are committed to offering our staff 'the best job you'll ever have' and have a diverse workforce in terms of gender, ethnicity, LGBTQ+ and social inclusion and are proud that our progress has been recognised by a gold award in the **TIDEmark** scheme (Talent, Inclusion and Diversity Evaluation).

In addition to our ISO14001 and ESOS accreditation, since 2020 all our offices have been powered by 100% renewable energy. We operate as a net zero carbon business and pledge to reduce our carbon footprint by 50% by 2025.

Our Clients & Customers

We help our clients, their employees, members, and customers make decisions that have real and direct consequences on their financial futures. We take this responsibility seriously and want to use our expertise to help clients make well informed choices. We recognise that helping our clients achieve their goals is what underpins our long-term success as a business.

Regardless of the market we're serving, our propositions focus on the ultimate beneficiary of our service – be that pension scheme members or individual savers.

We're uncompromising in our independent approach to finding the right solutions.

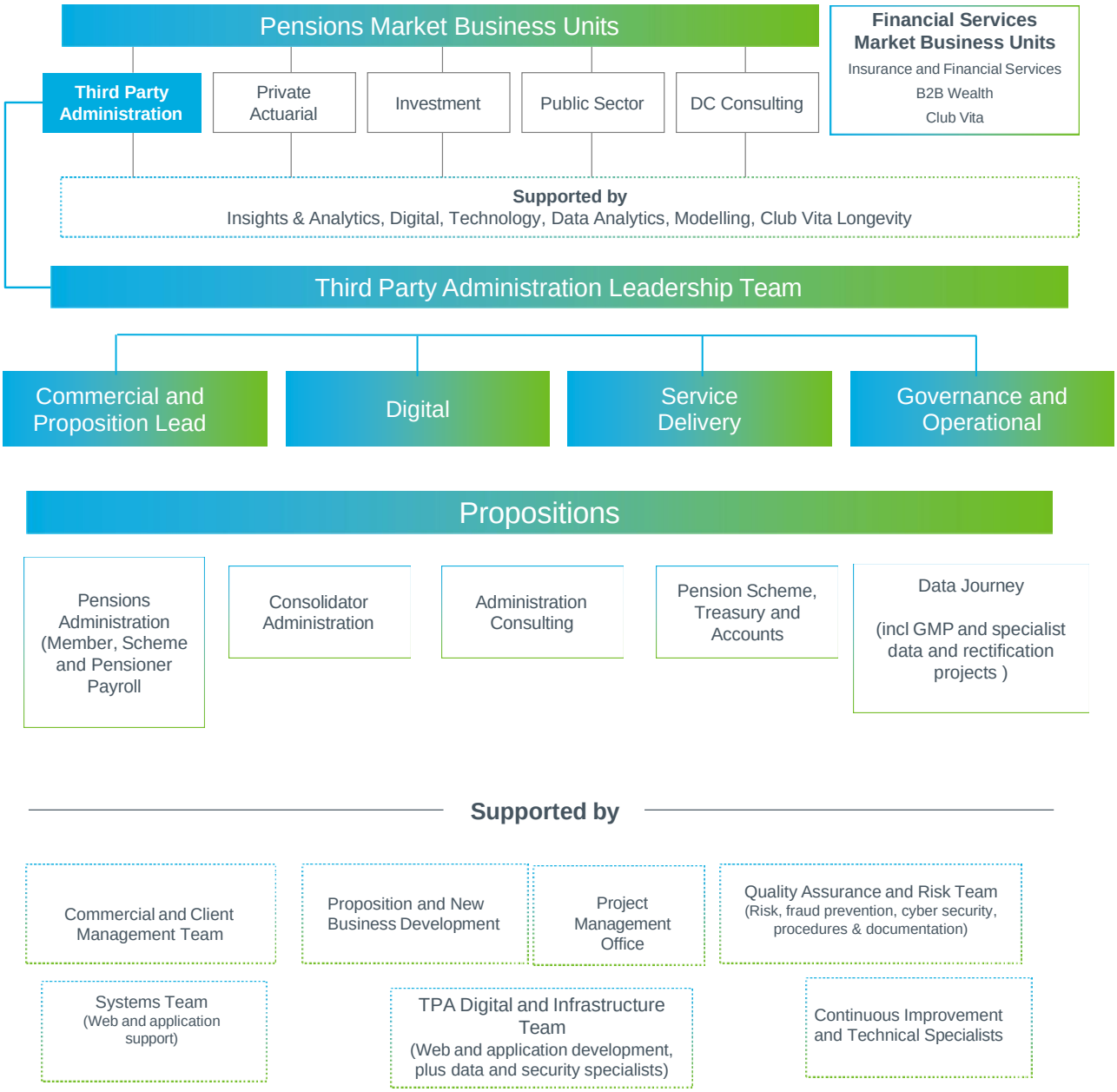
Through our annual Voice of Client Survey, we know that most of our clients value the service we deliver and the trusted relationships we hold. Indeed, most of our clients have been with us for over ten years.

3 Pensions Administration Business Unit

Administration Service Areas

The administration business unit has grown from our first client appointment with services being provided as part of our actuarial functions, to a business unit with a £14.8 million per annum turnover, employing over 270 staff, looking after over 78 clients' pension schemes from our four offices in London, Glasgow, Edinburgh, and Birmingham. We provide services for a wide range of clients with Defined Benefit, Defined Contribution, Hybrid and Career Average type arrangements.

The chart below outlines the service areas provided by our administration business unit:



In addition to our longer-term appointments, we draw on our experience in pensioner payroll, pension plan accounting and treasury services, plus general administration to offer one-off consultancy support to Hymans Robertson's existing clients and other organisations where in-house teams provide these activities.

We provide data cleanse services, GMPe, and benefit rectification services under our Data Journey proposition to help clients on their journey to buy-out.

Management Systems and Controls

Key elements of our management systems and controls to ensure quality of service for our clients include:

Checking

A self-check process guidance note is in place for administrators to ensure that all the required steps are followed and ensure there are no errors or omissions.

All work, whether routine or one-off, is controlled through the workflow process on our Civica Universal Pensions Management (UPM) system. It requires every item or process to be reviewed and authorised by an experienced Senior Administrator and / or member of the technical team before finalisation and issue.

All approvals for calculations and correspondence in respect of members are saved within the individual member record on UPM.

Service Level Agreements (SLAs)

Service standards are very important to our clients, us as administrators, but most importantly to the members we serve. Our SLAs are agreed with each client, and it is important to us that those agreed performance measures meet the schemes objectives and drive the best possible behaviours. We ensure that individual member needs are taken care of, and they receive the most appropriate service. Where industry wide resource issues have had an impact on SLAs in a minority of cases in the past twelve months, we've been proactive in bringing in extra resource from elsewhere across the practice and have communicated well with our clients to minimise any related complaints.

Operational Systems

Our pensions administration and pensioner payroll services are delivered using the UPM system, our operating platform for all the administration and pensioner payroll functions. The UPM system represents the latest generation of pensions administration software and provides us with the technology and operational tools that are necessary to deliver administration services in today's pensions environment.

The UPM software is installed, maintained, and developed by our own in-house team of system support analysts which forms part of our pensions administration business unit. Day-to-day operation and support for our administration teams is provided internally with secondary support taken from Civica, as and when necessary.

The software provides fully integrated administration and pension payroll functionality combined with sophisticated workflow and electronic document management facilities. UPM also supports internet access and self-service functionality for our individual scheme members and our client contacts.

Each UPM workflow is supported by a detailed process map held within the system and is set-up with embedded controls segregating the processing roles of an administrator and an authoriser. Automated workflow processes exist for all the administration and pension payroll tasks that we undertake.

Electronic document management is undertaken at our Glasgow office where we have centralised postage sorting and scanning. All incoming post and work items are sorted and scanned into UPM using procedures to comply with the requirements for BSI BIP 0008-1:2008 Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically.

Our Treasury and Pension Plan Accounting provider is Profund Aviary Professional.

Our Treasury and Pension Plan Accounting is all recorded through the electronic cashbook in Profund Aviary Professional.

Control Framework

The structure of the control framework within our administration business unit comprises formal monitoring at a management level, segregation of incompatible duties, and the design and implementation of appropriate preventative and detective controls. Our resources are managed within this framework to meet our quality standards and clients' expectations. Our operational controls are described in Section 9 of this report.

4 The Protection of Client Data

Introduction

Hymans Robertson has a long and successful history of safely handling sensitive and personal data. Our reputation depends upon the secure handling and processing of such data and therefore we invest heavily in suitable protection and mitigating any loss from occurring. We are continually seeking to ensure that our processes and systems remain fit for purpose.

We have given considerable thought to the most effective measures to ensure the safe handling of the data we hold on behalf of our clients. No-one can be 100% protected from cyber risk, but we do have the following measures in place to limit our exposure.

Governance

Our Managing Partner is a strong sponsor of information security and ensures that Hymans Robertson understands and supports this programme. Hymans Robertson has a dedicated Information Security Manager who reports into the Board at regular intervals to ensure that business risks, including information security, are appropriately identified and managed. The Information Security Board Sponsor has approved the Information Security Policy. Day to day responsibility for procedural matters, maintenance and updating of documentation, promotion of security awareness, liaison with external organisations, incident investigation, management reporting etc. rests with the Information Security Manager. Day to day responsibility for IT technical matters rests with the Head of IT.

Data Protection

Hymans Robertson has a data protection policy to which all staff are required to adhere. This keeps confidential member data secure and ensures compliance with the UK Data Protection Laws including the General Data Protection Regulation (GDPR). We are registered as a data controller with the Information Commissioner's Office.

Network Security

Hymans Robertson has a dedicated private circuit MPLS Wide Area Network (WAN) with full redundancy connecting all four offices.

Hymans Robertson also has multiple primary and back-up internet links protected by industrial grade firewall technologies. The firewalls are all configured using recommended best practice including anti-spoofing protection, stealth rules, port scanning, brute force protection and minimal opening of force with appropriate monitoring and alarming in place.

Internal and external communication is secured behind industry leading firewalls with policy rule enforcement preventing unsolicited intrusion from external sources to internal data. These firewalls employ packet inspection of all inbound and outbound traffic to spot suspect traffic, trapping and blocking it and logging all incidents, both positive and negative for review. The firewalls allow the segregation of individual computers and servers into different networks, which allows granular control over what computers and type of traffic that are permitted to and from the different servers. In addition, the firewalls provide the facility to log access to servers and protect against malicious internal activity.

We continuously assess vulnerabilities by means of an agent installed on every device in addition we do at least weekly scans of all our assets via an offbox vulnerability scanner. We also have real time monitoring of all assets for suspicious activity via our SIEM solution agent.

Hymans Robertson uses regularly updated anti-virus solutions on laptops which also checks for spyware and root kits. We use two anti-virus solutions that use both signature and artificial intelligence to detect malicious activity. We carry out monthly security patching and emergency patching as necessary.

Client data is located on protected servers which are stored in secure rooms and client data is also held in Microsoft Azure. All client data is encrypted at rest.

System Access and Passwords

All user access to Hymans Robertson information systems is authenticated by a unique user ID and password scheme assigned for everyone. Staff are prompted for MFA verification when connecting from an untrusted network.

Password complexity and history is enforced ensuring avoidance of easily guessed passwords and password re-use. As a minimum level of protection to all data held by Hymans Robertson, we use IPsec encryption for remote access; this is limited to domain joined devices that have been granted membership to specific groups. Third party remote access is limited to specific systems via a Citrix SSL session with 2 factor authentication and/or Site to Site VPN's (as required by the application).

Procedures for obtaining authorised access cannot be circumvented and users are aware of their responsibilities when accessing Hymans Robertson information systems and assets.

All users who require access to Hymans Robertson information systems must be assigned a unique set of access privileges that will allow them to access or modify only data required for their job function. Access privileges for users must be authorised by an appropriate manager.

Our joiner/leavers/movers process also prompts and manages user access.

Authorisations and changes to payments operates on a minimum of a 'two-person rule', and for BACS payments, this is further strengthened through required additional checks and authorisations. The release of most client documentation is subject to a similar 'peer-review' process.

Email Security

All external email is routed via the relevant cloud hosted gateways, which runs a series of checks including sender's reputation, presence of profanity, the validity of the recipient and whether the message is virus free. We block or rewrite malicious URLs based on reputation and in addition we have anti-domain spoofing.

Encrypted email recipients are required to create a secure encryption account, enabling them to access encrypted email delivered to their address. Access to the email is via a secure web browser allowing attachments and replies to be mailed directly back to the sender.

We use opportunistic TLS (Transport Layering Solution) AES 256 email encryption technology for all inbound and outbound emails, which ensures that all email information exchange between us and the client is automatically encrypted, thus requiring no user manual intervention.

Email borne viruses, spam and junk mail are filtered before they reach the network by a multi-layered protection system, whilst email encryption secures sensitive document transmission to and from target addresses when applicable.

Email and Web security

We have a DLP (data loss prevention) solution to prevent specific critical data from leaving the firm, all remaining data transfer is monitored and logged.

Secure file sharing

For sharing files containing bulk personal or confidential data we use a secure data portal called Sharefile. Sharefile encrypts files in transit and at rest. More information can be supplied about Sharefile on request.

Device security

Hymans Robertson laptops are encrypted with whole disk encryption, utilising a 256-bit encryption key. This prevents circumvention by malicious sources using key logging applications or malware and ensures that any data located on the laptop is fully encrypted and is unreadable unless accessed correctly. All laptops and mobile devices are further protected by a high-grade firewall.

We secure mobile phones through a combination of device encryption and application encryption which is enable using a 6-digit PIN passcode. Our Firm data is subject to application-level policies which secure data and prevents unwanted transfer or copying of data to unmanaged and unprotected systems. Condition access is used to enforce access control to data to compliant devices only.

Access to USB ports is locked down. Only IT service desk and specific use cases can access USB storage devices and all data is logged and monitored. If USB storage devices are required, then they are encrypted. Access management is controlled from a central database server for management, backup and unlocking in the event of a misplaced password.

Information Security Management System (ISMS)

Hymans Robertson is BS ISO/IEC 27001:2013 certified, which requires continual information security improvements and the whole Firm being subject to annual independent external audits by a registered ISO Accreditor.

The framework underpinning information security is the ISMS and associated manual, a requirement of ISO 27001. Key sections include:

Statement of Applicability – which documents how we comply with each of the stated controls within the ISO standard. This is used as the basis for both internal and external audits, to evidence that the control is happening in practice.

Policies - the individual information security policies we have include those covering:

Information Security	Acceptable Use	Access Control
Back-up	Clear Desk	Cloud Computing
Cryptographic Controls	Data Protection	Data Transfer and Encryption
Information Exchange	Malicious Software Protection	Mobile Computing
Network Systems Monitoring	Password	Secure Software Development
Security Incident Reporting	Software Piracy & Licensing	Virus Protection
Vulnerability Management		

All staff are expected to familiarise themselves with these policies, as evidenced by the annual staff declaration they must sign and our induction plan for new employees.

Web Application Security

Hymans Robertson offers clients a range of online applications. The applications allow on-line access for multiple users to stored information and are designed to use internet technology to minimise the risk of disclosure of confidential information by reducing the need to distribute paper, email attachments, or to carry sensitive documents on portable storage devices such as USB sticks or laptops.

Access is secured by an authentication method known as HymansID. This is based on Identity Server which uses OpenID Connect and OAuth 2.0 standards for ASP.NET core. Penetration tests are regularly carried out, at least once a year, by industry recognised, CREST, CHECK, CLAS (CESG Listed Adviser Scheme) agencies, to ensure our systems and data always remain at the forefront of information security best practice.

We have a Vulnerability Management Policy in place which applies to the online applications that we develop and maintain. We continually assess our applications for known vulnerabilities and in line with our Cyber Essentials certification.

On-line applications operate from a principal data centre, with the disaster recovery failover site operating from an alternative secure Hymans Robertson's data centre. Some application components may be hosted on cloud infrastructure in the EEA, which is configured in a resilient highly available manner.

All data centres and servers operate with at least dual redundancy components in the event of one failing, including two internet connections.

All publicly accessible entry points are protected by industry standard firewalls running intruder protection services.

Backups

A daily back-up of all required servers is run. All back-ups are encrypted, additional monthly backups are performed and stored on secure cloud storage.

Remote working

We operate a hybrid working model and all our staff are able to work from home securely. Our cyber security controls protect our home workers and our systems and data as they would in our offices. Only company-issued devices can connect to the network as we employ conditional access. We have a mobile computing policy which all staff must adhere to, which outlines our secure working practices outside of the office.

Remote access to our network is gained through a secure IPsec tunnel which uses multi-factor authentication. Access is denied if any of the relevant checks are violated.

Data retention

Hymans Robertson has a data retention policy which states how our data is managed, retained, and destroyed to be compliant with relevant industry standard and all relevant legal, regulatory and operational requirements.

Physical security

Physical access to our offices is restricted by swipe card/fob via a controlled reception area which have access barriers. Access to our physical IT systems is further restricted to selected individuals. This applies to each building and each floor. We have 24/7 building security and CCTV cameras at all external access points which are controlled and monitored by building management.

The data centres in all four locations have additional door code entry systems and only authorised members of our IT staff and the relevant Facilities Managers have access. The access lists are audited, and the codes are changed at frequent intervals.

In the office, desks are cleared at the end of each day and staff ensure that confidential information is locked away and their desk and surrounding area kept tidy, in line with our Clear Desk Policy.

All paper is disposed of securely using on-site shredding and specialist secure disposal services.

Third Parties

In selected instances Hymans Robertson uses the services of third parties who have more appropriate specialist skills or facilities, for some back-office and support activities.

As part of our due diligence processes at initial contract and ongoing reviews, information security is of paramount consideration, for both our own and especially client data e.g., historical records stored on and off-site. External solicitors have reviewed our potentially highest risk third party contracts and helped devise a model set of questions to ask suppliers with minimum acceptable expected responses and requirements to meet the information security policy. Hymans Robertson also employs specialist penetration testing companies to test and assess the security of its external facing applications annually. To minimise the risk of identity theft and fraud, specialist third party tracing bureau are used to validate addresses, and secure imaging systems are used to validate and prevent unauthorised changes to archived master documents and files retained by specialist archive companies.

Business Continuity

Hymans Robertson has a detailed Business Continuity Plan ("the Plan") which is aligned with quality standard ISO 22301. This Plan is divided into Emergency Response, Crisis Management, Business Recovery, and IT disaster recovery plans. The Plan also contains a pandemic plan. They exist to ensure the operation of the Firm can continue in the event of a disaster. The Business Continuity Plan is reviewed on a regular basis and exercises are carried out periodically by external consultants and our in-house business continuity team to test the effectiveness of the Plan and the staff involved in responding to a crisis. The focus is on keeping business critical processes and services running.

Hymans Robertson has advance planning for contingencies in place. We maintain suitable capacity at all times and minimise over-reliance on key individuals. Our experience is that this minimises the risks of disruption due to staff changes or absences.

Hymans Robertson has the ability for all staff to work from home. Our contingency plans also can adapt to relocate staff around its current offices. Our IT infrastructure has been constructed so that in a crisis, each office can operate independently from each other, and support recovery at other sites.

We ensure that we have no single points of failure by having the ability to replicate each office's systems. Business critical systems for each office are tested annually to ensure that they can be brought back online within the required recovery time for the key business functions.

We have a Cyber Incident Response Plan which works in conjunction with the Business Continuity Plan.

Staff Vetting

All staff employed and contracted by Hymans Robertson are subject to strict vetting. The offer of employment is conditional upon the outcome of these checks being satisfactory to the Firm. Checks include:

- Identity and validity to work in the UK
- Employment references covering the last 6 years
- Evidence of academic qualification and any relevant professional qualification
- Extended background checks that cover both financial soundness and criminal records
- All staff sign an annual declaration confirming their personal integrity and financial soundness, and indicate their understanding of our key internal policies
- All staff (including contractors and temporary staff) undertake information security awareness induction training

- Cleaners are vetted by their employing company as a minimum for valid visas, and are subject to a 10-year check into their history
- Building security officers are also vetted by their employing building management company and police checked. If non-UK resident, they are also vetted to ensure they have valid visas. Additionally, they have no access to our floors other than in an emergency.

Training

All staff undertake compulsory information security training every 12 months. All staff must sign the annual declaration to state that they will adhere to the information security policies. Regular information security communications are issued via different mediums. We conduct phishing exercises at regular intervals.

Security Incident or Data Breach Reporting

Information security incidents or data breaches are reported in accordance with our Security Incident Reporting policy and via our help desk function. High priority incidents are addressed immediately. We have a data breach response plan which we invoke if personal data is involved in an incident.

Clients will be notified as soon as possible if they are affected. Any notified incidents are discussed at the Board meetings, to ensure any lessons learned are actioned to prevent possible future occurrences.

An industry leading and ITIL-compliant help-desk system is used, which allows strong diagnosis and pro-active management of incidents.

Complementary User Entity Controls

We are responsible for the identification of Control Objectives relating to the provision of pension administration services, pension data audit and pension benefit audit services for pension scheme trustees 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 being achieved. The control procedures relating to pension administration activities cover only a portion of the overall internal control structure of each client. Each client must evaluate the control procedures detailed within this report in conjunction with the controls in existence at their own organisation.

Subservice Organisations

We no longer make use of Subservice Organisations for the provision of data migration work. The last project was delivered in September 2020.

Audits and Control Checks

Hymans Robertson undertakes a number of checks to ensure satisfactory adherence to its information security controls.

Independent external checks include:

- QMS International plc is our current independent ISO 27001 certifier. They conduct an annual review and test many controls at each of our locations.
- We have achieved Cyber Essentials accreditation.
- An independent annual internal controls assurance audit by a firm of Chartered Accountants on both our Third-Party Administration and Club Vita controls and systems – generating an AAF 01/20 Assurance Report. In addition to procedural operating controls, they report on information technology, covering (for the whole Firm) access rights to systems and data; integrity and resilience of the information processing environment; maintenance & development of systems hardware & software; and recovering from processing interruptions.

- An external consultancy company carries out an updated range of penetration tests covering an array of threats designed to identify areas of vulnerability. The tests can include network security testing, remote access and remote worker security testing and application security testing.

  The last test confirmed that Hymans Robertson's network perimeter is in line with good security practices; remote access testing was found to be well configured to prevent unauthorised access to the service, and applications testing demonstrated that systems had been configured to a high degree of security and integrity.

Any recommendations made by the external auditors or consultancies are immediately assessed and addressed in order of priority.

Internal checks include:

- Internal audits are undertaken at each of our locations on the controls within the ISO 27001 Statement of Applicability. This is a requirement to maintain ISO certification.
- Periodic information security risk assessments on selected information assets against a range of possible vulnerability threats.
- Managerial spot-checks are undertaken to ensure compliance with information security policies.

For any areas that may require strengthening, a risk treatment plan is developed and then implemented.

Summary

Hymans Robertson takes information security very seriously and has invested considerable time and money to ensure that your data is handled safely and securely. We will continue to seek improvements to processes and systems to prevent abuses. Whilst legal and regulatory requirements are of course a driving consideration, we have built a brand and reputation that we are proud of and extremely keen to maintain. You, our client, needs to know that we value and protect your data and are safe to do business with.

5 Report from the Partners of Hymans Robertson LLP

As Senior Management of Hymans Robertson ('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 sections 8, 9 and Club Vita fairly presents the Service Organisation's pension administration services throughout the period 1 February 2022 to 31 January 2023. In addition to the Control Objectives specified in AAF 01/20, the criteria used in making this statement were that the accompanying description:

i. Presents how the services were designed and implemented, including: the types of services provided, and as appropriate, the nature of transactions processed; the procedures, both automated and manual, by which User Entities' transactions were initiated, recorded, and processed; the accounting records and related data that were maintained, reported, and corrected as necessary; the system which captured and addressed significant events and conditions, other than User Entities' transactions; and other aspects of our control environment, risk assessment process, monitoring and information and communication systems, that were relevant to our Control Activities; and

ii. Includes relevant details of changes to the Service Organisation's system during the period; and

iii. Does not omit or distort information relevant to the scope of the services being described, while acknowledging that the description is prepared to meet the common needs of a broad range of User Entities and their auditors and may not, therefore, include every aspect of the services that each individual User Entity may consider important in its own 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 February 2022 to 31 January 2023. The criteria used in making this statement were that:

i The risks that threatened achievement of the Control Objectives stated in the Description were identified; and

ii. The identified Control Activities would, if operated as described, provide reasonable assurance that those risks did not prevent the stated Control Objectives from being achieved; and

iii. The Control Activities were consistently applied as designed.

This report covers the controls in place, and which were applied over the period 1 February 2022 to 31 January 2023, in accordance with the AAF 01/20 and ISAE 3402 framework.

We include a summary of the controls tested overleaf. There are some exceptions highlighted this year, four of which relate to the performance of the same control activity which we are planning to review as a standalone item ahead of next year's audit. Our business has been subject to a lot of change in recent months which we feel has contributed to this slight increase in the number of exceptions in this year's audit. Overall, though, we are pleased that there have been no material failings in our control environment.

Shirley Brown, Head of Third-Party Administration
Hymans Robertson
31 August 2023

Summary of Controls Tested

Pensions Administration

Control objectives	Number of Controls tested	Pages	Exception count
1 Accepting clients	5	27-30	No exceptions noted
2 Authorising and processing transactions	7	31-36	No exceptions noted
3 Maintaining financial and other records	9	37-42	2 exceptions noted
4 Safeguarding assets	16	43-50	2 exceptions noted
5 Monitoring compliance	7	51-55	2 exceptions noted
6 Reporting to clients	4	56-58	1 exception noted

Information Technology

Control objectives	Number of Controls tested	Pages	Exception count
7 Restricting access to systems and data	11	59-63	No exceptions noted
8 Providing integrity and resilience to the information processing environment	10	64-68	No exceptions noted
9 Maintaining and developing systems hardware and software	5	69-71	No exceptions noted
10 Recovering from processing interruptions	7	72-75	No exceptions noted

Club Vita

Control objectives	Number of Controls tested	Pages	Exception count
11 Restricting access to systems and data	7	76-78	No exceptions noted

Management Response to Exceptions Identified

This section provides detail of the exceptions identified during the audit period and the management response alongside each exception to explain and mitigate such exceptions in future.

Area	Control Number	Control Description	Exception	Management Response
3. Maintaining financial and other records	3.3.1	On a monthly basis, the monthly bank reconciliation is completed by a senior administrator or team leader who checks that all current and forthcoming incoming and outgoing payments are accounted for and signed off by a separate senior administrator or team leader. The date this has been completed is recorded on the Internal Controls Monthly reporting (MICR) control, which, in turn, is then reviewed and signed-off by the local administration manager.	For a sample of schemes, and for a sample of months, obtained the monthly bank reconciliation. Confirmed this was prepared and independently reviewed and that there were no discrepancies. However, not all instances of the sample tested were recorded in the corresponding MICR. For three schemes, unable to confirm that completion of the bank reconciliations had also been recorded in the MICR as this was not provided. Management confirmed the MICR had not been completed. Exception noted.	Management response: This is an internal reporting issue only, not an underlying process or governance issue. The cashflow analysis and bank reconciliations were all completed and authorised, and funds allocated as required. Scheme reporting to clients occurred too as required. However, confirmation of this was not recorded and signed off in a timely manner on the MICRs. We can confirm no actual breaches of the controls have occurred. Reporting via the MICRs impacts four controls (3.3.1, 3.4.3, 5.1.1 and 5.1.2). However, we can confirm all 4 four controls were completed in a timely manner. Therefore, no actual breaches of the controls have occurred.
	3.4.3	On a monthly basis, the defined contribution unit reconciliation is prepared by the administrator. The reconciliation is checked for completeness and accuracy through review of the administrator/senior administrator and signed off by the Team Leader. Upon completion, this is also recorded on the MICR which is reviewed and signed-off by each office administration manager.	For a sample of schemes, across a sample of months, obtained the DC unit reconciliation. Confirmed this was checked by an administrator/senior administrator and signed off by a team leader. Confirmed this was recorded in the corresponding MICR, however, noted that there were instances in the sample where the MICR was not provided and/or had not been completed appropriately.	This is an internal reporting issue only, not an underlying process or governance issue. Instances of the schemes sampled are Defined Benefit (DB) only. However, related cashflow analysis and bank reconciliations were all completed and authorised, and funds allocated as required for the DB sections of the scheme. The control did apply to one scheme (DB scheme with AVCs) only and appropriate reconciliations and client reporting was completed in the appropriate period. For all schemes, confirmation of control activity was not recorded and signed off in a timely manner on the MICRs. As per 5.1.2 no breaches have occurred.

Area	Control Number	Control Description	Exception	Management Response
4. Safeguarding assets	4.1.2	Hard copy documents are stored in dedicated filing areas when not in use at each office location and are readily accessible to the administration team.	Through observation, confirmed in one location that a filing system was in place, and whilst at times was unlocked, is on a floor where only TPA staff sit. Confirmed in a second location, the filing area is not restricted to the administration team as no locking/access mechanism in place, therefore, accessible to all staff.	All files have now been reviewed and either archived or destroyed. The related filing areas are unlocked each morning by Facilities team members, doors are closed through the day when not in use and the filing areas are locked again at the end of day. End of day procedures including guidance on storage, printing and mail handling are in place ensuring a clear desk policy is also applied at end of day.
	4.2.5	Cheque books are held in safe custody at a single central location and are only accessible by approved persons.	Through observation, it was noted that fob access to locked key box where filing cabinet key is stored in the central location was not restricted to approved persons.	We have replaced the fob access with new pin-pad access control that requires a 6-digit pin to be entered. Knowledge of this pin number is restricted to our Cash Management Team and the Business Unit Administrator plus two members of Facilities (for contingency and business continuity purposes). The password will be changed every six months or when a member of staff with access leaves the firm. This process has been documented and shared with the relevant team members. Where the fob access was in place, we can confirm that no risks materialised because of fob access not being locked down as the cash management team enter the payment information on to the accounting system, download the bank statements daily which they check against the accounting system and perform monthly bank reconciliations which would have identified any discrepancies.
5. Managing and monitoring compliance and outsourcing	5.1.1	Contributions are monitored monthly by the Administration team, and late or non-payment of contributions is recorded on the MICR report. Where there is a late or non-payment of contributions, this is reported	For a sample of DC schemes, across a sample of months and sites, confirmed that contributions had been recorded as received on the corresponding MICR. In one instance, the MICR was not provided, therefore, we were	This is an internal reporting issue only, not an underlying process or governance issue. For all schemes, monitoring and recording of contributions received was completed together

Area	Control Number	Control Description	Exception	Management Response
		promptly by the administration team to the scheme actuary and the client.	unable to confirm that the contributions monitoring had been correctly recorded. Exception noted. For the sample reviewed, there were no late or non-payment of contributions reported, therefore, this part of the control was not tested.	with the appropriate reconciliations and client reporting. However, confirmation of control activity was not recorded and signed off in a timely manner on the MICRs.
	5.1.2	Internal Controls Monthly Reports (MICR) are completed by each team leader to show they have checked all monthly tasks and legislative processes outside of BAU have been completed within the appropriate SLA. MICRs are submitted at the end of each calendar month to the local administration manager for review, with follow up where necessary, which is then further sign-off by the team leaders.	For three schemes, it was confirmed the MICR had not been completed and was therefore unavailable. The months selected to test the operating effectiveness of the control was May 2022, October 2022, and January 2023. Exception noted as unable to conclude the control is operating as described to confirm the objective has been met.	The MICRs have now been completed and authorised with a new process in place to ensure this occurs going forward. The MICR is an additional review across all our controls and is completed by the team leader and reviewed and signed by administration managers.
6. Reporting to clients	6.1.1	Quarterly (or at a frequency agreed with the client), administration reports are prepared by an Administrator and independently reviewed for completeness and accuracy, prior to issue to the client.	For a sample of schemes, across a sample of quarters (or as per occurrence) confirmed administration reports had been produced, reviewed, and issued to the client. It was noted that for one scheme, evidence of review was not appropriately documented, therefore, unable to confirm timeliness and completion of review.	This was a single instance of this approach to preparing an administration report and the appropriate team have been made aware of the correct process to apply to evidence this control to produce future reports.

6 Service Auditor Statement

The Service Auditor's Report has been prepared solely in accordance with terms of engagement agreed by the Senior Management of Hymans Robertson LLP ('the Senior Management') with RSM UK Risk Assurance Services LLP and for the confidential use of Hymans Robertson LLP ('the Service Organisation') and solely for the purpose reporting on the Control Activities in providing an independent conclusion on the Partners report set out on page 15 and 16 hereof. Our Report must not be relied upon by the Service Organisation for any other purpose whatsoever.

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

The Service Auditor's Report must not be relied upon by User Entities, their auditors or any other third party (together 'Third Parties') for any purpose whatsoever. RSM 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.

7 Service Auditor Report

RSM UK Risk Assurance Services LLP

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

Strictly Private & Confidential

REASONABLE ASSURANCE REPORT

The Partners
Hymans Robertson LLP
One London Wall
London
EC2Y 5EA

31 August 2023

Dear Sirs

INDEPENDENT SERVICE AUDITOR'S ASSURANCE REPORT ON THE CONTROL ACTIVITIES AT HYMANS ROBERTSON LLP

This report is made solely for the use of Senior Management, as a body, of Hymans Robertson 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 8 March 2023.

SCOPE

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

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

The Service Auditor's Report is designed to meet the agreed requirements of the Service Organisation and particular features of our engagement determined by their needs at the time. The Service Auditor's report should not therefore be regarded as suitable to be used or relied on by any other party wishing to acquire any

rights against RSM UK Risk Assurance Services LLP for any purpose or in any context. Any party other than the Service Organisation which obtains access to this report or a copy and chooses to rely on the Service Auditor's Report (or any part of it) will do so at its own risk. To the fullest extent permitted by law, RSM UK Risk Assurance Services LLP will accept no responsibility or liability in respect of this report to any other party and shall not be liable for any loss, damage or expense of whatsoever nature which is caused by any person's reliance on representations in this report.

We permit the disclosure of the Service Auditor's Report, in full only, to current and prospective User Entities of the Service Organisation using the Service Organisation's pension administration services and related information technology ('User Entities'), and to the auditors of such User Entities, to enable User Entities and their auditors to verify that the Service Auditor's Report has been commissioned by Senior Management 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 from page 1 to 14 and the accompanying Partners Statement set out on page 15 and 16, including the completeness, accuracy, and method of presentation of the description and the Directors Statement;
- providing the Service Organisation's 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 25 and 26, include the internal Control Objectives developed for the service organisation as set out in the ICAEW Technical Release AAF 01/20 and ISAE 3402.

SERVICE AUDITOR'S RESPONSIBILITIES

Our responsibility is to express an opinion on the fairness of the presentation of the Description and on the suitability of the design and operating effectiveness of the Control Activities to achieve the related Control Objectives stated in that Description based on our procedures. We conducted our engagement in accordance with International Standard on Assurance Engagements 3000 (Revised), and ICAEW Technical Release AAF 01/20. Those standards and guidance require that we comply with ethical requirements and plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the Description is fairly presented and the Control Activities were suitably designed to achieve the related Control Objectives stated in the Description.

An assurance engagement of this type also includes evaluating the overall presentation of the Description and the suitability of the Control Objectives stated therein, and the suitability of the criteria specified by the Service Organisation and described from page 1 to 14. Our work involved performing procedures to obtain evidence about the presentation of the Description of the Service Organisation activities or system and the design and operating effectiveness of those controls. Our procedures included assessing the risks that the Description is not fairly presented and that the Control Activities were not suitably designed or operating effectively to achieve the related Control Objectives stated in the description.

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

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

INHERENT LIMITATIONS

The Service Organisation's Description is prepared to meet the common needs of a broad range of User Entities and their auditors and may not, therefore, include every aspect of the Service Organisation's pension administration activities and 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 Partners' Statement on page 15 and 16:

a) the Description on pages 1 to 14 fairly presents the Service Organisation's pension administration activities and related information technology as designed and implemented throughout the period from 1 February 2022 to 31 January 2023;

b) the Control Activities related to the Control Objectives stated in the Description were suitably designed to provide reasonable assurance that the specified Control Objectives would be achieved if the described Control Activities operated effectively throughout the period from 1 February 2022 to 31 January 2023; and

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 February 2022 to 31 January 2023.

DESCRIPTION OF TESTS OF CONTROLS

The specific controls tested and the nature, timing and results of those tests are detailed on pages 27 to 78.

RSM UK Risk Assurance Services LLP

RSM UK Risk Assurance Services LLP
London

31 August 2023

8 Summary of Control of Objectives

This section provides summary information on the design, description, and operation of the control procedures for the administration, accounting, information technology and Club Vita functions, as described in the Partners' report for Hymans Robertson.

Pensions Administration

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.

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

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

3 Maintaining Financial and other Records

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

Receipts of contributions, in accordance with Scheme rules and legislative requirements, are monitored against required timescales.

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 sponsors are accurate and complete and provided within required timescales.

Annual reports and accounts are prepared in accordance with applicable laws and regulations.

Information Technology

7 Restricting Access to Systems and Data

Physical access to computer networks, equipment, storage media and program documentation is restricted to authorised individuals.

Logical access to 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.

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

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.

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

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. are authorised, tested, approved, and implemented.

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

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

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

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

The physical IT equipment is maintained in a controlled environment.

Club Vita – Information Technology

11 Restricting Access to Systems and Data

Logical access to Club Vita computer systems, programs, master data, transaction data and parameters, including access by administrators to applications, databases, systems, and networks, is restricted to authorised individuals within the Club Vita operations in accordance with the Club Vita System Access Control Policy. Logical Client Web Access to Club Vita master data, transaction data and reports is restricted to authorised individuals at Clients in line with the Club Vita Client Setup Policy.

Not applicable control objectives

It should be noted that the following objectives are not applicable to Hymans Robertson pension administration processes:

- 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.

Hymans Robertson no longer makes use of Subservice Organisations for the provision of data migration work; however, we will continue to monitor our processes to ensure that relevant controls are in place should they become relevant.

9 Control Objectives and Control Activities

1 Accepting Clients

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

Process Description

Following a successful administration services tender process, new clients are required to agree and sign a standard Letter of Appointment. This letter allows the formal transition exercise to commence. Where necessary, Data Sharing agreements may be put in place as an interim measure to allow work to start until the formal Master Service Agreement is in place.

Where an appointment is made for Hymans Robertson to provide full services, the appointment documentation will normally be collated on behalf of the lead consultant, with all services responsible for providing their relevant Service Orders for inclusion in the Master Services Agreement If the appointment is for administration only, the Master Service Agreement will be collated by a responsible person in the Third-Party Administration Business Unit.

Once collated, the Master Service Agreement will be issued in draft format, along with our standard Terms and Conditions document, to allow the client and their legal advisers the opportunity to comment on the terms contained therein. On agreement, a final version of the documentation is issued to the client for signing. All Master Service Agreements must be countersigned by an authorised representative of the Firm, normally at Partner level or above. The Master Service Agreement must be signed and in place before administration services can commence.

Although transition work can take place under the initial Letter of Appointment, failure to finalise and agree the Master Service Agreement and Terms and Conditions may result in a delay in the commencement of the services.

Control Activity	Auditor Testing and Results
1.1.1: Letter of Appointment, Master Service Agreement and, if applicable, a Data Processing agreement are completed for each new client to ensure that all stages of the process are followed and documented	1.1.1: For a sample of new clients, obtained the letter of appointment, master service agreement and Data processing agreement. Confirmed that each had been completed and retained. No exceptions noted.

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

Process Description

All new clients are accepted through a documented process which covers the stages from responding to the initial invitation to tender; completion of the necessary due diligence for compliance with anti-money laundering regulations proposal for services; presentations and site visits and finally the installation exercise following appointment.

The processes followed and respective controls are recorded within the following documents:

- Tender review process
- Formal proposal for services
- Client verification and anti-money laundering form
- New client set up form
- New client installation checklist and detailed project plan and
- New client installation timeline

The structured methodology and installation process for a new client is referred to in the sections below.

The scheme is set-up using information derived from the proposal for services, the trust deed and rules, member announcements, explanatory booklets, membership data and hard copy records and other information that is made available. All data required for the setup of the new scheme is requested from the incumbent administrator and the client using template installation data request letters and forms.

Membership data is subjected to validation testing and data mapping, which structures the data in alignment with the structures on UPM, using data conversion software. A calculation test harness is used for testing calculations. Thorough testing of this data on the UPM test platform is undertaken prior to email sign-off by a lead member of each relevant service area. The sign-off email is saved to UPM as part of the change control release process and is a precondition to releasing the data to the Live UPM environment.

Control Activity	Auditor Testing and Results
1.2.1: A new client installation checklist or detailed project plan is completed for each new client to ensure that all stages of the process are followed and documented. AML checks are completed by the administration team and retained. Upon completion, an email is prepared by an analyst in the systems team confirming checks have been completed before being reviewed and signed off by a team leader in the administration team, prior to data being released into the Live UPM environment.	1.2.1: For a sample of new clients, obtained the detailed project plan. Confirmed this was completed in all stages. Confirmed AML checks had been completed and retained. Confirmed email had been issued prior to data being released in to Live UPM environment. No exceptions noted.

Process Description

The live data load is received and input to the data conversion software prior to processing on the UPM test platform. Testing of the live data is undertaken in the same manner as that of the client test data load, and reconciliation reports are run and reviewed. The mapping of membership data is also checked against hard copy member prints where these are made available by the incumbent administrator.

The live data change control workflow goes through peer review approval before proceeding to the live release stage. The testing and test sign-off is carried out by someone other than the person performing the data migration and test sign-off is always required from the administration team and (if applicable) the payroll team as part of the review process.

For defined contribution schemes, individual member investment elections and unit holdings are included in the data mapping exercise from the previous administrator. For new defined contribution schemes, member elections are recorded from the members' joining information and application forms.

Unit reconciliations are requested from the previous administrator at the closure of their records to ensure a clean start point for our unit holdings from the live services date.

Control total testing is carried out following data load exercises to test numbers of members by status type and financial totals such as salary, contribution, and defined contribution unit histories.	
Control Activity	**Auditor Testing and Results**
1.2.2: As needed, control total testing is carried out by the administration team, following data load exercises to ensure that numbers of members by status type and financial totals such as salary, contribution and defined contribution unit histories are uploaded accurately. Upon completion, data validation is authorised by the administration team leader. For new Defined Contribution Schemes, Unit Reconciliations are carried out by the administration team and subject to review by an administration team leader in UPM.	1.2.2: For a sample of new clients, confirmed data validation was completed and authorised by administration team leader. No exceptions noted. There were no new DC schemes in the reporting period, therefore, the last part of the control was not required to operate. Management confirmed the control remains as described.

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

Process Description

The project installation process involves various resources within the administration business unit, dependent upon the scope of and range of administration services that are to be provided. The process may involve project management resource from outside the administration business unit to manage the project.

The set-up of a scheme involves the allocated administration team, system support team and the local office administration manager. Where the client has agreed additional services such as pensioner payroll, annual report and financial statements and cash management, the Pensions Finance Manager will oversee the set-up of these services.

The resources refer to a detailed installation checklist and a detailed project plan throughout the set-up of a new client. This is supported by an installation timeline which identifies key tasks to be undertaken within a recommended timetable. A sign-off control is required on completion of each section of the installation checklist. The project manager also updates the project plan with a date of completion to confirm that all relevant tasks were completed. The system support team develop their integrated work plan covering technical issues from the initial receipt of client test data to the live processing date.

The process involved is demonstrated in the steps outlined below:

- As part of a new client installation, a client contact is established for receipt of periodic communication.
- Receive final closing balances, detailed trial balance, bank reconciliations, bank statements and all lead schedules for audited accounts for the previous reporting period from the previous scheme administrator/in-house accounts team.
- Review and reconcile back all documents received from previous scheme administrator/in-house accounts team to the audited accounts for previous reporting period.
- Defined Benefit Investment Cash transactions are reconciled through the Trustee bank account to the independently received investment manager confirmations.

• Map transactions from previous scheme administrator schedules to internal accounting system, post audited closing trial balance at the previous reporting period and roll forward to the go live date. • Post cashbook transactions from previous reporting period to go live date, complete monthly bank reconciliations and agree back to previous scheme administrator versions. • Once completed and reconciled, this is communicated to the client using the agreed method and contact.

Control Activity	Auditor Testing and Results
1.3.1: Each section of the installation checklist is signed off or a detailed project plan is updated with a completion date to ensure that steps detailed above have been completed.	1.3.1: For a sample of new schemes, confirmed that a checklist or project plan was in place. Confirmed that the plan had a completion date. No exceptions noted.

Process Description
Member data originating prior to the installation of the UPM system is back scanned and stored at the member record level as required.

Control Activity	Auditor Testing and Results
1.3.2: For new clients, member data originating prior to the installation of the UPM system is back scanned and stored at the member record level as required	1.3.2: For a sample of new clients, confirmed that for one take-on, member data was required to be back-scanned to UPM. Through observation, confirmed that hard copy document was attached and stored at the member record level. No exceptions noted.

2 Authorising and Processing Transactions

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

Process Description

Team leaders and senior administrators are aware of the due dates for contribution receipts such that they will contact a client if not received in line with the agreed schedules and in advance of the 19th of the month following deduction.

The administration team receives notification from the client of contribution funding into the trustee bank account monthly. This is supported with backing information to confirm the amount of contributions being remitted and, for defined contribution schemes, a breakdown of the contributions for each member to enable investment allocation.

On receipt of funds, the cash book is updated.

Defined contribution funds are invested with the investment manager within three working days of receipt of clean data and payment.

Following investment, a contract note is received from each investment manager. Some clients have Straight Through Processing in place with the Investment Managers.

There is a transaction-by-transaction validation test built within UPM which is completed in real time. This validation tests the total investment amount, the unit prices supplied on the contract note or updated via STP and number of units purchased on a transactional basis. If the test output does not match, UPM will automatically generate an on-screen warning message to investigate further.

There's also a range of data validation tests which are run retrospectively monthly. These are applied across all DC membership and highlight any areas for query or investigation. Each of the validation processes are authorised and signed-off in UPM by a team member who has the appropriate authorisation. In addition to the UPM controls and validations, timely and accurate investment of monthly contributions and transfers in is reviewed as part of the Monthly Defined Contribution Cash analysis. This analysis is performed outside UPM, and any unverified amounts identified by this analysis are logged, reviewed, and then referred to the administration teams for action.

For defined benefit schemes, contributions received are compared against known outgoings and contingency levels; surplus funds are subsequently invested in accordance with the client's instructions. All transactions involving the movement of funds are controlled through the cash management authorisation process controls identified elsewhere in objective 4.2. We note that the initial review is prepared and authorised and if there is a surplus, the investment is usually authorised by the Trustee. Some investments, however, will not be authorised by the Trustees as we may have a pre instruction form/ agreement in place to invest if this is done on a regular basis.

Control Activity	Auditor Testing and Results
2.1.1: Upon receipt of contributions, for Defined Benefit schemes, the administration team will check they are received as expected. On a monthly basis the team will action a cash flow analysis to check the amount on account and guaranteed income received, will cover expected outgo. This will result in either an investment or disinvestment being required. The cashflow will be actioned by an	2.1.1: For a sample of schemes, across a sample of months, obtained the cash flow analysis and confirmed receipt of contributions. Confirmed cash flow had been prepared by the administrator and reviewed by senior administrator and agreeing amount to invest/disinvest, as covered in controls 3.4.1 and 3.4.2.

administrator, with a senior administrator (or above) checking the cashflow and agreeing the amount to invest / disinvest. The investment / disinvestment is then arranged. For defined contribution schemes, contributions received are reconciled by the Hymans DC team with a retrospective check against expected amounts versus amount received/invested and allocated to options against funds/units etc and returns received from investment managers on allocations.	Monitoring of contributions is also covered in control 5.1.1.

Process Description

Transferred-in benefits are processed in the same way as a receipt of contributions and the DC transfer-in UPM process performs the same validations across the member record. The transfer-in is invested in line with member instruction and the investment instruction is issued to the investment manager within 3 working days (3 working days is best practice) of receipt of reconciled funds into the Trustee bank account. Once the contract-note is received the UPM record is updated with the unit holdings, UPM data updates are authorised and the member is notified that the transfer is complete, where their units are held and the value of those units. Targets in UPM however, are not set up in line with best practice, so this process relies upon the administration team to monitor receipt of transfer and manage within 3 working days. There's additional daily reporting built into UPM to highlight all ongoing DC transfer-in cases and the current stage for each case. This report is generated and automatically issued each day for Team Leaders to manage timely investment of transfer-in payments.

Control Activity	**Auditor Testing and Results**
2.1.2: Transfer-in benefits are processed in UPM by an administrator and authorised by a separate member of the team. The investment is actioned within best practice of 3 working days of receipt of reconciled funds in line with SLAs. Once complete the transfer in details are checked and authorised by an independent administrator on UPM to ensure they align with what is expected from the transfer in originally quoted and is accurately recorded on UPM.	2.1.2: For a sample of transfer-in benefits, inspected UPM and confirmed that transfer-ins were processed by an administrator and authorised by a second administrator. Confirmed investment actioned within SLA. Confirmed transfer-in details were authorised by an independent administrator in UPM. No exceptions noted.

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

Process Description

Each UPM process has an embedded control making it obligatory that another administrator authorises the members' investment instructions. A switch of members' funds between investment options and/or investment managers must be instructed by either the members or the Trustees for life styling or investment rebalancing. Member instructions are processed on receipt of a valid completed switch form or online request. Scheme/Plan life styling is completed in line with client service orders.

Following receipt of an investment switch instruction a UPM Switch Matrix or Investment Change process is created at member level on the UPM record. Updates are then made to the member record, in line with

instruction, and an instruction is issued to the appropriate investment manager. Once the contract note is received updates are made to the member record to reflect the units sold and purchased. A switch must be actioned and completed within 5 working days of receipt of the request and the appropriate SLA is recorded within UPM. Lifestyle switch processing and individual member switches between investment options are undertaken through the embedded workflow controls within the UPM system and actioned within 5 working days. Sign-off is performed and recorded within UPM. The life styling process is automatically generated on 1st of every month unless this falls on a weekend in which case the process starts on the following Monday. The 5 working day SLA is dependent on receipt of contributions, therefore, if contributions are being invested, at the time the life styling process is generated, the investment of contributions takes priority and life styling begins once the contribution process has been completed	
Control Activity	**Auditor Testing and Results**
2.2.1: Switches are processed in UPM as and when required for a member by the administration team and authorised by a separate member of the team. A switch is actioned within 5 working days of receipt of the request. Following the switch, the updates are recorded in UPM which are checked and authorised accordingly by a senior administrator. Upon receipt of contract notes and updating the member record, the sign-off is performed and recorded within UPM by a senior administrator/team leader.	2.2.1: For a sample switches, inspected the UPM and confirmed that this had been processed by a member of the administration teams and authorised by a second member of the team. Confirmed the switch was actioned within 5 working days. Confirmed switch updates and signoffs were completed by the senior administrator/team leader in UPM. No exceptions noted.

2.3 Benefits payable and transfer values are calculated in accordance with scheme rules and relevant legislation and are paid within agreed timescales.
Process Description Benefit payments and transfer values are processed by the administration team having detailed knowledge of the operation of a scheme and are either calculated through automated processes set up in the UPM system or undertaken manually prior to being incorporated into the UPM workflow process. Each UPM process has an embedded control making it obligatory that another person authorises the transaction on-line at the member record level. Any manual calculations are required to be independently checked, and where appropriate peer reviewed, as part of the authorisation stage of the workflow process. Evidence of the checking and peer review is recorded by the authoriser. The manual calculation documents are scanned into the UPM system and stored on the individual members' records. All calculations are checked by a team member with the appropriate authorisation before payment processing. Transfer payments are paid within 2 months of receipt of completed transfer discharge forms. Retirement lump sum payments are paid no later than 12 months after the member becomes entitled to the relevant pension. Death payments are paid within 2 years of the Trustees receiving notification of the death of the member. Appropriate letters to accompany each payment are produced either automatically from the UPM system or manually, and copies are held within the system at the member record level.

Control Activity	**Auditor Testing and Results**
2.3.1: Each UPM process is authorised by another person online at the member record level. As needed, manual calculations prepared by the administrator are required to be independently checked, and where appropriate peer reviewed, as part of the authorisation stage of the workflow process. Automation checks are required to be checked at a frequency which has been agreed by the client. Evidence of the checking and peer review is recorded by the authoriser for both manual and automated checks as appropriate. All calculations are checked before processing any benefit payments. Appropriate letters to accompany each payment are produced and copies are held within the system at the member record level.	2.3.1: For a sample of benefit payments, inspected UPM and confirmed evidence of checking and peer review for manual and automated calculations as appropriate. Where a manual calculation was used, confirmed this had been prepared by an administrator and independently checked as part of the UPM workflow. Inspected the member letters produced, confirmed this matched the payment and held at member record level. No exceptions noted.

Process Description

Where members require future review of benefits (to ensure that quotes and options available to members are issued on a timely basis) including members reaching normal retirement date, State pension age, cessation of dependent's/ill-health pensions, controls are in place to launch a Future Review Process in advance. A date is entered into the relevant Future Review field within the UPM record (this is either done manually by an administrator and then authorised by another member of the team, or, automatically as part of a UPM process such as retirement process or death process). When the Future Review date is reached the relevant process to review and update the UPM record is created, actioned, and authorised within UPM.

Alternatively, for those clients who have adopted the warmup letter process this letter will be sent to the member in advance of their normal retirement date.

Control Activity	Auditor Testing and Results
2.3.2: Where members require future review of benefits (to ensure that quotes and options available to members are issued on a timely basis) including members reaching normal retirement date, State pension age, cessation of dependents'/ill health pensions, Future Review code is run daily in the UPM database to determine the relevant members; from which processes are then started automatically by the Scheduler.	2.3.2: For a sample of members reaching retirement, inspected documentation, and confirmed that retirement quotes and options had been sent in a timely manner. No exceptions noted.

Process Description The death in service process has an embedded control that ensures that death claims are made to the insurer where death benefits are insured. The UPM process has mandatory routes within it for the administrator to follow to create documents to claim the Life Assurance benefit from the insurer and/or Defined Contribution benefit from the investment manager. The documents are checked and authorised by another member of the administration team with a full audit trail recorded within the UPM process.	
Control Activity	**Auditor Testing and Results**
2.3.3: The UPM process has mandatory routes within it for the administrator to follow to create documents to claim the Life Assurance benefit from the insurer and/or DC benefit from the investment manager for a death in service, should one occur. The documents are checked and authorised by another member of the administration team with a full audit trail recorded within the UPM process	2.3.3: For a sample of death in service benefit payments, inspected the supporting documentation and confirmed that the claim had been processed by an administrator, independently reviewed by a second administrator and this was authorised in UPM. No exceptions noted.

Process Description UPM retirement and death processes have embedded controls to ensure that new pensioners and beneficiary pensioners may only be created because of processing retirements or deaths for existing active, deferred or pensioner members. In addition, to create a new pensioner or beneficiary pensioner payroll record, authorisation must be carried out at the administration stage and the payroll member creation stage by a member of the administration team and a member of the payroll team respectively.	
Control Activity	**Auditor Testing and Results**
2.3.4: As needed, to create a new pensioner or beneficiary pensioner payroll record, authorisation must be conducted at the administration stage by a member of the administration team within UPM and subsequently a member of the payroll team (where we administer the Trustee bank account), for a record to be created in UPM. Where we do not administer the Trustee bank account, a payroll form will be issued to the client to commence payments for the member accordingly.	2.3.4: For a sample of new pensioners/ new beneficiaries obtained evidence to support approvals in place to create member payroll records. Confirmed approved payroll form in place where required and that appropriate sign offs in UPM. No exceptions noted.

3 Maintaining financial and other records 3.1 Member records consist of up to date and accurate information	
Process Description Members' records and supporting documentation are held electronically within the UPM system. Records and changes are updated daily through ad hoc instructions generated by the members or authorised client contacts, and annually through renewal and annual increase exercises. Personal member details are processed by a member of the administration team and peer reviewed by a senior administrator.	
Control Activity	**Auditor Testing and Results**
3.1.1: A change of address or change of personal details, such as name, are processed and updated on UPM by an administrator in the administration team and peer reviewed by an independent administrator.	3.1.1: For a sample of member detail changes, obtained the supporting documentation and inspected the UPM audit trail to confirm checks were completed, changes processed by an administrator and peer reviewed by an independent administrator. No exceptions noted.

Process Description Daily at each office location all incoming pension administration post and work items are sorted and scanned into UPM to comply with the requirements for BSI BIP 0008-1: 2008 Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically. The post handling and scanning follows a defined procedure including the use of scan batch controls. Post is dealt with at our Glasgow office where it is sorted and scanned into UPM to comply with the requirements for BSI BIP 0008-1: 2008 Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically. Original documentary evidence of identity and address is required before benefits can be settled. Original certificates received are scanned, and additionally, controlled using a register to record relevant details including the date of receipt and return by recorded delivery. If a member is requesting a settlement of benefits, we will require them to provide the current list of Identify and Verification (ID&V) documents via a secure link plus some additional ID&V documentation as we will not be able to have sight of the original documents in line with our normal procedures and controls. Once scanned into UPM, items are allocated to an administration team, appropriately indexed, and assigned for processing. Each work item is linked to a workflow process having an embedded control segregating the processing roles of an administrator and an authoriser. Daily monitoring of work-in-progress and prioritisation is undertaken by each team leader or senior administrator. Workflow analysis is monitored at a management level and through the Monthly Internal Controls Report (MICR). Annual renewal exercises for active members and deferred members where relevant and pension increases for pensioner members are undertaken through specific workflow processes within the UPM system. For pensioner payroll records, a bulk tax code change process is interfaced with data files provided by HMRC.	
Control Activity	**Auditor Testing and Results**
3.1.2: Pension increases are processed annually. Pension increases to be applied are prepared and applied in UPM by the scheme administrator. This is then subject to review for completeness and accuracy by a senior administrator or team leader	3.1.2: For a sample of schemes, obtained UPM audit trail and supporting evidence to confirm that the annual pension increase exercise had been completed. Confirmed that this has been prepared by an administrator in UPM and reviewed by an

and authorised in UPM. Pension increases letters are produced and issued to the members upon completion. An audit trail is maintained in UPM to document the review and approval process.	independent administrator. Confirmed pension increase letters produced and issued. No exceptions noted.

Process Description Membership statistics for each scheme are extracted from UPM, reconciled, reviewed by a senior member of the administration team, and reported to clients as part of the quarterly administration reporting.	
Control Activity	**Auditor Testing and Results**
3.1.3: Quarterly (or as agreed with client), member statistics for each scheme are extracted from UPM by the administrator and reconciled to the previous quarters report, and member movements report to confirm completeness and accuracy. This is then independently reviewed by a senior member of the administration team and reported to clients in the quarterly administration reports issued to Trustees/clients.	3.1.3: For a sample of schemes, and for a sample of quarters (or at the frequency agreed with the client), obtained member statistic reconciliations. Confirmed reconciliations had been reconciled to previous reports. Confirmed this had been reviewed by a senior member of the administration team and was included in the corresponding administration reports. No exceptions noted.

Process Description Reconciliation of membership records also occur annually for the Annual Report and Financial Statements document which is signed-off by the clients and their external auditors. The reconciliation of membership is peer reviewed by a senior member of the administration team.	
Control Activity	**Auditor Testing and Results**
3.1.4: Quarterly (or as agreed with client), membership reconciliations for each scheme are extracted from UPM by the administrator and reconciled to the previous quarters report, and member movements report to confirm completeness and accuracy. This is then independently reviewed by a senior member of the administration team and reported to clients in the quarterly administration reports issued to Trustees/clients.	3.1.4: For a sample of schemes, obtained membership reconciliations. Confirmed reconciliations had been reconciled to previous reports. Confirmed this had been reviewed by a senior member of the administration team and was included in the corresponding administration reports. No exceptions noted.

3.2 Requests to change member records are validated for authenticity Process description
Process Description The administration team regularly receives requests to update member personal details, such as address, direct from the member or their employer (if Active/Active-Deferred). If the request is received from the employer, it is updated to match the information provided. If the request is received from the Scheme member there are several steps the administrator must take, in following our document process, to verify the member and the legitimacy of the data change request before

it is updated on the member record.

Upon receipt of a change of address request via telephone where the address held is not 'gone away' and the member is not a pensioner / beneficiary pensioner the details are taken, and the record updated. If the address held is gone away, or the member is a pensioner / beneficiary pensioner, then we will ask the member to send in evidence of their new address and confirm this must be one of the items shown in the list 2 below. In these cases, we may take the new address and write out to the member to confirm the items we require before an update to the record is made. For any change in personal details, such as marital status and change in name, then before an update to the record is made.

For all cases where a benefit is to be set up / paid, then we will request proof of name, proof of address and proof of bank account. Proof of bank account, however, is not required for transfer out cases.

Once the additional ID&V documents are received, if they fit the requirements of our process, we can update the member UPM record. All updates are authorised within UPM by a separate member of the team. If the member's address was recorded as 'gone away' due to having received returned correspondence, we also perform an IDU desktop search via Lexis Nexis on the new address details given. If this returns a 'pass', we can update the record. If a 'refer' or 'fail' is returned this is escalated internally or further investigation.

If a member has requested to change their address as part of their retirement process, we request the ID&V documents required and additionally perform the IDU desktop search via Lexis Nexis as part of the retirement process.

All results for all IDU checks are recorded within the UPM record.

Following the implementation of an updated process to allow additional checks made for overseas ID&V since September 2021, we continue to use ID-Pal, which is an app for members to download and use.

Control Activity	Auditor Testing and Results
3.2.1: As needed, ID checks are performed by the administration team. ID is verified and copies of the ID are loaded to the UPM record before updates are made to the UPM record and before benefits are paid.	3.2.1: For a sample of changes to member details and benefit payments, obtained evidence of ID checks and confirmed this was completed prior updated and to payments made and documented in UPM. No exceptions noted.

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

Process Description

Contributions and benefit payments are recorded in the cash book on the day the transaction occurs.

Bank reconciliations are undertaken and checked monthly, with the reconciliation date entered onto the MICR. This report is reviewed and signed-off by each office administration manager who sample checks where necessary.

Control Activity	Auditor Testing and Results
3.3.1: On a monthly basis, the monthly bank reconciliation is completed by a senior administrator or team leader who checks that all current and	3.3.1: For a sample of schemes, and for a sample of months, obtained the monthly bank reconciliation. Confirmed this was prepared and

forthcoming incoming and outgoing payments are accounted for and signed off by a separate senior administrator or team leader. The date this has been completed is recorded on the MICR control, which, in turn, is then reviewed and signed-off by the site administration manager.	independently reviewed and that there were no discrepancies. However, not all instances of the sample tested were recorded in the corresponding MICR. For three schemes, unable to confirm that completion of the bank reconciliations had also been recorded in the MICR as this was not provided. Management confirmed the MICR had not been completed. Exception noted. *Management response: This is an internal reporting issue only, not an underlying process or governance issue. The cashflow analysis and bank reconciliations were all completed and authorised, and funds allocated as required. Scheme reporting to clients occurred too as required. However, confirmation of this was not recorded and signed off in a timely manner on the MICRs. We can confirm no actual breaches of the controls have occurred.*

3.4 Investment transactions, balances and related income are completely and accurately recorded in the proper period	
Process Description For a Defined Benefit scheme, investment transactions arise out of the cash management process where funds more than outgoings and contingency are identified. These funds are invested in accordance with clients' instructions and are recorded in the cash book. Controls within the cash management process include surplus funds are signed-off by a checker, an instruction is sent to the investment manager advising of investment, the payment to the investment manager is undertaken through the segregated control processes within the electronic banking system identified below, and the bank instruction form to invest the money is signed off by two authorised signatories.	
Control Activity	**Auditor Testing and Results**
3.4.1: On a monthly basis, surplus funds are identified during the cash flow analysis and recorded in the cash flow spreadsheet. The cashflow will be actioned by an administrator, with a senior administrator checking. If there is a surplus, an investment is made; otherwise, there is a disinvestment. For investments / disinvestments, an instruction form is usually raised by the administrator and checked by a senior administrator. Once this is completed the form will be signed by two authorised signatories. Depending on the client this may be Hyman's signatories or the trustees.	3.4.1: For a sample of schemes, across a sample a sample of months, obtained the cash flow analysis spreadsheet. Confirmed this had been reviewed. Where an investment/disinvestment had been made, confirmed an instruction form had been raised and appropriately approved by two authorised signatories. No exceptions noted.

Process Description A disinvestment transaction is controlled in a similar manner, but an order instruction is raised, authorised by another member of the team, and issued to an investment manager. The cash book is updated on receipt of funds.	
Control Activity	**Auditor Testing and Results**
3.4.2: Following the monthly cash flow reconciliation (refer to control 3.4.1), there will be a monthly disinvestment of investments, as appropriate. An order instruction is raised by the administrator, authorised by a senior administrator or team leader, and signed by two authorised signatories and issued to an investment manager.	3.4.2: For the sample in control 3.4.1, where a disinvestment was made, confirmed the order instruction was raised, authorised, signed by two authorised signatories, and issued to the investment manager. No exceptions noted.

Process Description For a Defined Contribution scheme, the transfer of members' funds between investment options and lifestyle switching is undertaken through the embedded controls within UPM processes. This is covered under objective 2.2. Bank reconciliation controls operate and are detailed elsewhere in this report. Defined Contribution unit reconciliations are carried out monthly or in line with the reporting cycles of relevant investment managers where monthly reporting is unavailable. These unit reconciliations are reported as having been completed in the MICR.	
Control Activity	**Auditor Testing and Results**
3.4.3: On a monthly basis, the administrator prepares the defined contribution unit reconciliation. The reconciliation is checked for completeness and accuracy through review of the administrator/senior administrator and signed off by the team leader. Upon completion, this is also recorded on the MICR which is reviewed and signed-off by each site administration manager.	3.4.3: For a sample of schemes, across a sample of months, obtained the DC unit reconciliation. Confirmed this was checked by an administrator/senior administrator and signed off by a team leader. Confirmed this was recorded in the corresponding MICR, however, noted that there were instances in the sample where the MICR was not provided and/or had not been completed appropriately. Exception noted. *Management response: This is an internal reporting issue only, not an underlying process or governance issue. Instances of the schemes sampled are Defined Benefit (DB) only. However, related cashflow analysis and bank reconciliations were all completed and authorised, and funds allocated as required for the DB sections of the scheme.* *The control did apply to one scheme (DB scheme with AVCs) only and appropriate reconciliations and client reporting was completed in the appropriate period. For*

	all schemes, confirmation of control activity was not recorded and signed off in a timely manner on the MICRs.

4 Safeguarding Assets 4.1 Member records are securely held, and access is restricted to authorised individuals process description	
Process Description Member and scheme data are stored electronically on the UPM system. Access requires layered passwords, each layer being controlled and administered separately. Access levels are granted in accordance with job responsibilities.	
Control Activity	**Auditor Testing and Results**
4.1.1: Access requires layered passwords, each layer being controlled and administered separately.	4.1.1: Observed a user accessing the UPM application and noted that passwords were required, and that access within the application was restricted based on the user's role (layered). No exceptions noted.

Process Description Hard copy documents are stored in dedicated filing areas when not in use at each office location and are readily accessible to the administration teams within TPA. Entry per location is with a pass to restrict access.	
Control Activity	**Auditor Testing and Results**
4.1.2: Hard copy documents are stored in dedicated filing areas at each office location and are readily accessible to the administration teams.	4.1.2: Through observation, confirmed in one location that a filing system was in place, and whilst at times was unlocked, is on a floor where only TPA staff sit. Confirmed in a second location, the filing area is not restricted to the administration team as no locking/access mechanism in place, therefore, accessible to all staff. Exception noted. *Management response: All files have now been reviewed and either archived or destroyed. The related filing areas are unlocked each morning by Facilities team members, doors are closed through the day when not in use and the filing areas are locked again at the end of day. End of day procedures including guidance on storage, printing and mail handling are in place ensuring a clear desk policy is also applied at end of day.*

Process Description Historical hard copy member data is archived and held in secure storage with our approved off-site suppliers relevant to each office location.	
Control Activity	**Auditor Testing and Results**
4.1.3: Historical hard copy member data is archived and held in secure storage with our approved off-site suppliers relevant to each office location.	4.1.3: Through discussions with management confirmed the archiving process in place for hard copy member data. Obtained and confirmed a valid contract is in place with a secure storage supplier. No exceptions noted.

4.2 Cash in Scheme bank account is safeguarded, and payments are suitably authorised process description	
Process Description Client bank accounts are established in the name of the trustees or the scheme with a restricted list of Hymans Robertson signatories to effect payments and transactions within each account. Clients have the option to specify upper signing limits. Upper signing limits will be operated based upon client instructions and requiring client representatives to authorise payments above those agreed limits. There is a listing of authorised personnel with access rights, which is reviewed annually. Only those staff who are team leader upwards or are of equivalent level and do work within the admin teams, are permitted to authorise payments.	
Control Activity	**Auditor Testing and Results**
4.2.1: All Hymans bank accounts have the same Hymans signatories. A full update review is done yearly with all signatories signing the same mandate template and forwarded to the relevant bank for confirmation. New signatories are added, and leavers removed from the mandate on an ad hoc basis throughout the year via an authorised letter authorised by two authorised signatories from the mandate to each bank.	4.2.1: Obtained the annual update reviews and confirmed this had been completed and forwarded to the relevant bank for confirmation. Where a new signatory had been added, confirmed authorised letter by two authorised signatories from the bank mandate was in place. No exceptions noted.

Control Activity	**Auditor Testing and Results**
4.2.2: Following client instructions to make payments, investments or disinvestments, client representatives within Hymans are authorised to make such payments, investments, or disinvestments.	4.2.2: Testing of this control was covered in controls 2.2.1, 3.4.1, 3.4.2 and 4.2.4.

Process Description

Each client bank account relating to defined benefit will be established with a lower and upper limit on account balances. These limits are reviewed and monitored as part of the monthly bank account reconciliation process. An automated warning process applies when these limits are exceeded to trigger review and any action that may need to be taken.

Control Activity	Auditor Testing and Results
4.2.3: A warning process applies when the established lower and upper limits of bank accounts are exceeded which triggers a review and any action that may need to be taken. A cashflow alert via email is received from the cash management team and is issued to team leaders to deal accordingly. The checks are performed monthly via a cash management team administrator performing the monthly payroll reconciliations for the Trustee bank account.	4.2.3: For a sample of schemes, across a sample of months, through review of the monthly cashflow and bank reconciliation pack, where triggered, confirmed that a cashflow alert via email was received from the cash management team and issued to team leaders to deal accordingly. Confirmed this check is performed monthly. No exceptions noted.

Process Description

Where a client account is established with our relationship bank, electronic banking facilities are available, and these are operated with appropriate authorisation and segregation. The bank allocates the Trustee bank account to our on-line workstation number. When written confirmation of allocation is received, the accounts team liaises with the allocated administration and cash management team who will operate the client account and set-up the cashbook and record keeping details.

- To undertake an electronic payment four segregated processing steps are required;
- Administration team member prepares input backing documentation;
- Separate administration team member checks supporting documentation;
- Separate administration team or cash management team member checks inputs;
- Verification of the payment instruction is completed by a third person, independent of the administration process; and
- Final authorisation of the payment is completed by a fourth person, again independent of the administration process.

Electronic transmission of a payment using an authentication device is undertaken as a separate process. Separate members of the team prepared and authorised the transaction. After transmission, the submitted documentation and payment processing details are returned to the administration team. A transmission confirmation is retained as a separate record.

Control Activity	Auditor Testing and Results
4.2.4: As needed, to undertake an electronic payment four segregated processing steps are required: • Administration team member prepares input backing documentation.	4.2.4: For a sample of member payments, obtained the supporting documentation to the payment made. Inspected the backing documentation and confirmed that that this had been prepared by an administrator, checked by a second administrator who input into the banking portal. Confirmed the input matched to the payment instructions. Confirmed checks in place by

• Separate administration team member checks supporting documentation and inputs on to online banking portal. • Separate administration team or cash management team member checks inputs on to online banking portal. • Verification of the payment instruction on the online banking portal is completed by a third person, independent of the administration process. • Final authorisation of the payment on the online banking portal is completed by a fourth person, again independent of the administration process.	cash management team and that the payment instruction was authorised by an independent person and that the payment was released in the banking portal by a further independent individual. No exceptions noted.

Process Description The alternative to making an electronic payment is cheque processing. Cheque books are held in safe custody in our Glasgow office and are only accessible by approved persons. Cheque signatories are identified on authorised bank mandates which are updated as required, and a copy retained at the Glasgow office.	
Control Activity	**Auditor Testing and Results**
4.2.5: Cheques books are held in safe custody at a single central location and are only accessible by approved persons.	4.2.5: Through observation, it was noted that fob access to locked key box where filing cabinet key is stored in the central location was not restricted to approved persons. Exception noted. *Management response: We have replaced the fob access with new pin-pad access control that requires a 6-digit pin to be entered. Knowledge of this pin number is restricted to our Cash Management Team and the Business Unit Administrator plus two members of Facilities (for contingency and business continuity purposes) and the password will be changed every six months or when a member of staff with access leaves the firm. This process has been documented and shared with the relevant team members.* *Where the fob access was in place, we can confirm that no risks materialised because of fob access not being locked down as the cash management team enter the payment information on to the accounting system, download the bank statements daily which they check against the accounting system and perform monthly bank reconciliations which would have identified any discrepancies.*

Process Description The cash management team prepares a cheque. The prepared, but unsigned cheque together with supporting transaction and cash management documentation is submitted to two authorised cheque signatories for signing. The signed cheque is issued, and the documentation is returned to the cash management team who scans a copy of the payment documentation on to the member record within the UPM system.	
Control Activity	**Auditor Testing and Results**
4.2.6: Cheque payments follow the same process as electronic payments in that they are prepared by an administrator and authorised by a senior administrator before being passed to cash management. The supporting documentation is passed to cash management where a member of the team will write the cheque before being passed to a senior administrator in cash management for review. Two authorised Hyman's signatories then sign the cheque.	4.2.6: For a sample of cheque payments, obtained the backing documentation and confirmed this was prepared by an administrator and reviewed by a senior administrator. Inspected the cheque and confirmed this was prepared and checked by the cash management team. Confirmed the cheque was authorised by two signatories. No exceptions noted.

Process Description Cheque register logs in respect of cheque payments received, are maintained as part of the post opening duties, at our Glasgow office which logs payee, amount, scheme and date banked. Cheques are scanned onto the UPM record then passed to the Cash Management team, for banking, on the day received to ensure prompt paying in.in line with FCA Client Asset Sourcebook ("CASS") rules.	
Control Activity	**Auditor Testing and Results**
4.2.7: Cheque register logs in respect of cheque payments received, are maintained as part of the post opening duties, at one single location which logs payee, amount, scheme, and date banked. Cheques are scanned onto the UPM record then passed to the Cash Management team, for banking.	4.2.7: Inspected the cheque register log and confirmed this is maintained. Confirmed this details payee, amount, scheme, and date cheques have been banked. For a sample of cheques received, confirmed these had been scanned onto UPM and banked. No exceptions noted.

Process Description

At the end of a calendar month each team is required to submit to the site administration manager their MICR specifying the dates on which bank reconciliation were performed. The report is reviewed by sample checking, follow-up where necessary, and sign-off. All sign-off is now performed via electronic signature with the administration team doer, checker and administration manager/operations lead providing final electronic sign-off.

Bank reconciliations are performed monthly. The centralised cash management unit undertakes reconciliation of their cash management accounts. A sign-off stamp of both the doer and the checker is recorded in addition to the date of reconciliation.

Control Activity	Auditor Testing and Results
4.2.8 Where an administration team has retained the cash management function, they perform the monthly bank reconciliation. See control 3.4.1. A sign-off stamp of both the doer and checker is recorded in addition to the date of reconciliation. This date is then recorded in the MICR.	4.2.8: Refer to control 3.4.1 where testing of this control has been covered.

Process Description

Where a client has elected for a pensioner payroll service, this service is administered by the central payroll processing unit, using the payroll module within the UPM system. Segregation of duties is demonstrated by the central payroll unit undertaking the administration processing to the creation of a BACS file for each payroll group, and the designated group of senior staff located in each office, undertake the payment processing and transmission of each BACS file. A manual check is performed to compare each payroll total to the previous month and differences of more than 10% are investigated.

Control Activity	Auditor Testing and Results
4.2.9: A payroll administrator prepares the payroll for a given client each month which is approved and authorised off by a senior payroll administrator. Any variances such as increases or decreases will be investigated and reported on by a payroll administrator and submitted in the payroll reconciliation report for authorisation by a senior payroll administrator.	4.2.9: For a sample of schemes, across a sample of months, obtained the monthly payroll reconciliation pack and confirmed this was prepared by a payroll administrator a reviewed by a senior administrator. Confirmed that any variances were investigated and resolved. No exceptions noted.

Process Description

Controls evident on documentation arising from the UPM system together with the relevant payroll reconciliation sheet are by a duly completed quality sign-off stamp, which also identifies the BACS file name and creation date. The PAYE reconciliation is prepared by an administrator within the payroll team. This is then peer reviewed and authorised by a senior administrator within the payroll team.

Control Activity	Auditor Testing and Results
4.2.10: Controls evident on documentation for the monthly pension payroll arising from the UPM system together with the relevant payroll reconciliation sheet are approved by a duly completed quality sign-off stamp, which identifies the BACS file name and creation date.	4.2.10: For the sample of schemes and months in control 4.2.9, confirmed that the payroll reconciliation sheet was completed with a quality sign-off stamp, and BACS file name and creation date were identified. No exceptions noted.

Process Description

Client payrolls have been processed individually and directly from the relevant client trustee bank account without the use of a payroll clearing account. The payment of PAYE to HMRC is undertaken electronically before the statutory deadline each month from each client bank account.

Control Activity	Auditor Testing and Results
4.2.11 Payment of PAYE follows standard payment process (refer to control 4.2.7) with the payment to HMRC undertaken electronically before the statutory deadline each month from each client bank account. PAYE reconciliations and corresponding PAYE payments are both performed as part of the monthly payroll process.	4.2.11: For the sample of schemes and months in control 4.2.9, confirmed that the PAYE reconciliation and payment were performed as part of the monthly payroll process. No exceptions noted.

4.3 Periodic reports to The Pensions Regulator and HMRC are complete and accurate process description

Process Description

We provide an annual update to HMRC each 31 January for any Scheme Events that require reporting as part of regulatory guidelines, such as those members who have breached Lifetime Allowance in the prior year. The data is extracted from UPM, using a specifically designed report. The data extract is then reviewed by the administrator to identify which members require reporting. Once the members are identified, the data is entered into a submission report through HMRC Pension Schemes Online. Prior to submitting the report, the inputs are checked by a senior member of the team and the client authorises the submission before being finalised.

A further annual submission is a Scheme Annual Return. Whilst TPA may not be required to submit this for all clients, we will be required to provide information regarding TPA activities and membership data.

Additionally, we update a quarterly Accounting For Tax submission, per Scheme, if any members have received a refund of contributions or have tax to pay if their retirement benefits exceed the permitted Lifetime Allowance. The payments for which are paid to HMRC prior to the deadline in the following quarter.

All tax submissions are prepared by a team administrator, then reviewed and authorised by a senior member of the team before final submission on the HMRC online platform. Once submitted, the

administrator is then able to make the relevant payment to HMRC.

Monthly we issue PAYE information, via our Payroll team, to HMRC regarding each of the pensioners paid per client. This data is generated using a dedicated UPM process, which calculates the tax due to HMRC and generates an RTI submission file to be sent to HMRC in order that each member record is kept up to date with HMRC. The reconciliation is prepared by an administrator within the payroll team. This is then peer reviewed and authorised by a senior administrator within the payroll team.

The automated RTI submission is part of the rigid process within UPM and the administrator running the payroll cannot advance beyond this stage without a positive submission receipt. If the process submission fails, then it is investigated and corrected before the submission is resent.

Upon receipt of a successful RTI submission the submission receipt is saved to the payroll documents by the administrator and the process moves on to the next stage. An automated e-mail is also sent to the TPA shared inbox confirming whether the RTI submission was successful/unsuccessful.

Once the tax calculations are complete, a request for payment is then sent to the cash management team for each of the clients for which we pay pensions. The cash management team then make a PAYE payment to HMRC for each client.

Control Activity	Auditor Testing and Results
4.3.1: PAYE reconciliations and corresponding PAYE payments are performed monthly. The PAYE reconciliation is prepared by an administrator within the payroll team. This is then peer reviewed and authorised by a senior administrator within the payroll team.	4.3.1: This control is performed as part of the monthly payroll processing and has been covered in control 4.2.9.

Control Activity	Auditor Testing and Results
4.3.2: The automated RTI submission is part of the rigid process within UPM and the administrator running the payroll cannot advance beyond this stage without a positive submission receipt. If the process submission fails, then it is investigated and corrected before the submission is resent.	4.3.2: Through observation confirmed that the administrator running the payroll cannot advance within UPM without a positive submission receipt. For the sample of schemes and months in control 4.2.9, confirmed the RTI submission had been completed. No exceptions noted.

5 Managing and monitoring compliance and outsourcing 5.1 Receipts of contributions, in accordance with Scheme rules and legislative requirements, are monitored against required timescales	
Process Description Each administration team monitors the receipt of contributions in accordance with each scheme's Schedule of Contributions/Payment Schedule and in accordance with each client's established business unit. Payment dates and payment methodologies will vary from client to client. Any late or non-payment of contributions are included on the MICR and communicated to the Scheme actuary and client and monitored at management level. Administration teams operate checking processes to identify expected payment dates for each client individually. Non-payment or late payment is reported promptly by the administration team to the scheme actuary and the client. Cash Management team record receipt of contribution payments within the cashbook ledgers noting amounts and dates of payment.	
Control Activity	**Auditor Testing and Results**
5.1.1: Contributions are monitored monthly by the Administration team, and late or non-payment of contributions is recorded on the MICR report. Where there is a late or non-payment of contributions, this is reported promptly by the administration team to the scheme actuary and the client.	5.1.1: For a sample of DC schemes, across a sample of months and sites, confirmed that contributions had been recorded as received on the corresponding MICR. In one instance, the MICR was not provided, therefore, we were unable to confirm that the contributions monitoring had been correctly recorded. Exception noted. For the sample reviewed, there were no late or non-payment of contributions reported, therefore, this part of the control was not tested. *Management response: This is an internal reporting issue only, not an underlying process or governance issue.* *For all schemes, monitoring and recording of contributions received was completed together with the appropriate reconciliations and client reporting. However, confirmation of control activity was not recorded and signed off in a timely manner on the MICRs.*

Process Description
MICRs are completed by each team leader to show they have checked all monthly tasks and legislative processes outside of BAU have been completed within the appropriate SLA. The MICR identifies the due dates for key internally reportable items for each team. Actual event dates are completed by each team leader and reports are submitted at the end of each calendar month to the site administration manager for review, follow-up where necessary and sign-off by the team leaders. The reportable items include the dates for receipt and processing of contributions for defined contribution schemes, defined benefit schemes, monthly contribution investments and lifestyle switch processing.

The Client Service Delivery Lead would only be required to review and sign the report should an exception be identified or if an item required further investigation. Should the site administration manager not be available to review a sign the report, either an administration manager from another site may step in to perform this action or alternatively the Client Service Delivery Lead.

Control Activity	Auditor Testing and Results
5.1.2: MICRs are submitted at the end of each calendar month to the local administration manager for review, with follow up where necessary, which is then further signed-off by the team leaders.	5.1.2: For a sample of schemes, across a sample of months, obtained the MICR. For three schemes of the sample, management confirmed the MICR had not been completed and was, therefore, unavailable. Unable to conclude the control is operating effectively as described. Exception noted. *Management response: The MICRs have now been completed and authorised with a new process in place to ensure this occurs going forward. The MICR is an additional review across all our controls and is completed by the team leader and reviewed and signed by administration managers.*

5.2 Pensions administration activities are governed by service level agreements that are authorised and subject to regular review. Service performance is regularly monitored and assessed against the standards set out in service level agreements
Process Description The scope and high-level delivery of services is agreed with each client at the appointment and new scheme installation stage. Any subsequent change to requirements or services are discussed and agreed with each client as and when required and before implementation. The service level agreement (SLA) is amended accordingly and signed by both Hymans Robertson and the client. All business as usual (BAU) day to day administration work recorded within the UPM system is allocated a target completion date and various reporting tools via the UPM system are available to team leaders to monitor completion and performance standards. Any issues are escalated by the team leader to the team administrators to ensure completion of work.

Control Activity	Auditor Testing and Results
5.2.1: The scope and high-level delivery of services is agreed with each client at the appointment and new scheme installation stage. Any subsequent change to requirements or services are discussed and agreed with each client as and when required and before implementation. The SLA is amended accordingly and shared with the client.	5.2.1: Based on discussions with management it was confirmed that there were no changes to scheme SLA's in the reporting period, therefore, the control did not require to operate. Management have confirmed the control remains as described.

Process Description

Once the live services have commenced, day to day work is recorded within the UPM system and its integrated workflow control tool. Administration staff and team leaders work directly from electronic work trays within the system and can monitor and sort work in accordance with due dates for completion and levels of priority.

All work recorded within the UPM system is allocated a target completion date, using SLAs that are embedded into UPM, and various reporting tools are available to monitor completion and performance standards. Details of workflow processing are included within the quarterly administration reporting which is explained elsewhere in this document.

Control Activity	Auditor Testing and Results
5.2.2: Administration staff and team leaders work directly from electronic work trays within the system and can monitor and sort work in accordance with due dates for completion and levels of priority. Administration team leaders review workloads for their team members daily. All business as usual (BAU) day to day administration work recorded within the UPM system is allocated a target completion date and various reporting tools via the UPM system are available to team leaders to monitor completion and performance standards. Any issues are escalated by the team leader to the team administrators to ensure completion of work. SLA is monitored by the administration team/team leaders and reported to the client through the quarterly administration reports (or frequency agreed with the client)	5.2.2: Through observation of UPM and discussions with management, confirmed that the administrator staff and team leader use UPM work trays. Confirmed office that work is allocated in UPM and target completion is in place with reporting tools available. For a sample of schemes and a sample of quarters, confirmed that SLA reporting is in place in the administration reports. No exceptions noted.

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

Process Description

A formal and documented Risk Event reporting process exists nationally across our business. All employees are trained in the procedures and have access to the reporting guidelines.

Control Activity	Auditor Testing and Results
5.3.1: All employees are trained in the risk events procedures both at induction and then on an annual refresher basis. This consists of training delivered by a Quality Assurance team member with guidance available for reference afterwards.	5.3.1: For a sample of new starters, obtained the induction checklist and confirmed that training had been completed. Inspected refresher training process and management confirmed annual refresher training is in place by the QA team. No exceptions noted.

Process Description

The administration teams complete a template form after discussion with the Administration manager which is forwarded to the TPA Quality Assurance team who assess the nature of the event and decide whether Legal advice is required, whether the event constitutes a Risk to Hymans Robertson or whether the matter can be managed within the TPA business unit. This decision is based upon the materiality (financial and/or reputational) and the incidence of the type of event.

The information is input to the Risk Event database and either Legal or Risk are notified via this database when input is required.

The Legal Team and Risk & Compliance Team have access to this database. Other access is restricted to the Quality Assurance team who manage all Events through to completion.

Any transaction errors or complaints are treated as Risk Events and are recorded upon the Risk Event Database in accordance with our standard documented procedure.

GDPR events are logged and managed via the Privacy Hub in accordance with Firm wide procedure.

Control Activity	Auditor Testing and Results
5.3.2: Where a risk event is identified, a formal report is completed by the client team and submitted to the Quality Assurance Team. The report is reviewed, and the event rated (1 through to 5 being most critical) and logged on the risk events database. The Quality Assurance team will then assist the teams to identify remedial actions, advise on reporting to the client and review draft responses back to the members. Once the issue has been resolved, the case is closed on the risk event database.	5.3.2: For a sample of risk events, obtained the completed formal reports. Confirmed these has been reviewed, event rated, and logged on the risk events database. Inspected evidence of remedial actions and resolution. No exceptions noted.

Process Description
Risk Events are rated 1 through to 5 with 5 being Critical (e.g., a loss of key systems/facilities for more than a business day, the issue affects more than 25% of members, clients, or staff and/or high potential for customer detriment, potential financial loss of >£1m). The Quality Assurance team (and Legal or Risk as required) work with the client team and the Operations Lead (for Risk Events rated 3 or higher) to determine the corrective action to be taken in each case. The parties will also agree the extent to which the Client Director should be involved in the resolution of the event. They provide advice to the client team; review communication material as required and ensure the progress of each case is managed to a resolution. The Operations Lead is updated verbally monthly on the ongoing position of events by the Quality Assurance team and which events have been escalated to Legal or Risk.

Control Activity	**Auditor Testing and Results**
5.3.3: Material risk events (rated 3 or above) are reported to the TPA Head of Business Unit for oversight purposes mainly but also to agree if involvement is required in the risk event resolution by the Operations Lead, the related Client Director, or any other senior management / senior parties.	5.3.3: For a sample of material risk events (rated 3 or above), confirmed that the events were reported, and Operations Lead/Client Director involved as per Risk Event Matrix. No exceptions noted.

6 Reporting to clients 6.1 Periodic reports to participants and scheme sponsors are accurate and complete and provided within the required timescales	
Process Description Quarterly (or at a frequency agreed with the client) administration reports to clients are compiled for each scheme using various sources of data which are entered onto a specific scheme template. Each report is prepared and checked prior to issue. Reports are usually issued to coincide with client trustee meetings, however not always for some clients. The reports provide commentary on the administration services provided during the reporting period together with statistical details on work completed and in progress; financial summaries and extracts from the cashbooks; and where relevant, copies of individual member feedback forms which have been received by the administration teams.	
Control Activity	**Auditor Testing and Results**
6.1.1: Quarterly (or at a frequency agreed with the client), administration reports are prepared by an Administrator and independently reviewed for completeness and accuracy, prior to issue to the client.	6.1.1: For a sample of schemes, across a sample of quarters (or as per occurrence) confirmed administration reports had been produced, reviewed, and issued to the client. It was noted that for one scheme, evidence of review was not appropriately documented, therefore, unable to confirm timeliness and completion of review. Exception noted. *Management response: This was a single instance of this approach to preparing an administration report and the appropriate team have been made aware of the correct process to apply to evidence this control to produce future reports.*

Process Description Annual benefit statements are produced for individual members, and these provide information of the members' benefit entitlements across a range of scenarios, typically covering retirement, death and early leaving. The design and content of the benefit statements will depend upon the scheme type and the requirements of each client. The operational control to produce annual benefit statements arises through the automated workflow processes within the UPM system. Benefit calculations are completed through the automated calculation routines within the UPM system.	
Control Activity	**Auditor Testing and Results**
6.1.2: On an annual basis, benefit statements are produced by the scheme administrator through the automated workflow processes within the UPM system. Benefit calculations are completed by the	6.1.2: For a sample of schemes, confirmed that annual benefit statements are produced through the automated workflow processes within the UPM system which are completed by the administrator

administrator through the automated calculation routines within the UPM system and subject to review by a senior administrator or team leader. A copy of the benefit statement is saved on the member record.	and approved by the senior administrator or team leader. Confirmed that a copy of the benefit statement was saved to the member record on UPM. No exceptions noted.

Process Description

Statutory Money Purchase Illustration (SMPI) details are calculated using the DC Illustration System. The illustration output from the DCI System is then independently verified by a checking spreadsheet built by Hymans Actuarial SMPI team, which follows the TM1 standard practice. The DC Team compare and then verify the system outputs against the spreadsheet outputs.

If there are no changes in the year to Defined Contribution funds, Scheme structure; contribution band rules or life styling matrix, the calculations do not need to be updated and then verified by the Actuarial SMPI team. If there are changes, the Actuarial SMPI team will verify the outputs.

Each year, the Hymans Defined Contribution team update the annuity rates and fund returns. Following this, the Defined Contribution team generate the Defined Contribution Illustration (DCI) outputs and check any outliers. The checking spreadsheet is then signed-off by the Actuarial SMPI team.

The SMPI statements are not signed-off by the Actuarial SMPI team unless there have been any significant changes to the structure or wording within the statement.

Control Activity	**Auditor Testing and Results**
6.1.3: Annual SMPI statements are calculated by the administration team using the DC Illustration System which is independently verified through a checking spreadsheet built by the Actuarial SMPI team. The checking spreadsheet is then checked by a senior administrator or team leader and finally signed-off by the Actuarial SMPI team.	6.1.3: For a sample of DC schemes, obtained the checking spreadsheet and confirmed this had been prepared by the admin team and checked by a senior member of the team and final sign off by the Actuarial SMPI team. No exceptions noted.

6.2 Annual reports and accounts are prepared in accordance with applicable laws and regulations

Process Description

A scheme's Annual Report and Financial Statements (in both draft and final versions) are prepared by the accounts team, primarily from information supplied by the scheme's investment manager(s) and the relevant internal cash management system. A software package is used to merge the sources of data to produce a trial balance.

A member of the accounts team inputs the trial balance and member data into a statutory compliant Annual Report and Financial Statements template document. This provides the draft document which is reviewed by another member of the accounts team prior to audit by the scheme's external auditors. The preparer and reviewer sign off the final draft so that it links to the control and testing. As part of the statutory audit, the final version of the Annual Report and Financial Statements is approved by the scheme's trustees. The external auditors will then approve the Independent Auditor's Report and the Independent Auditors' Statement about Contributions.

The final version of the Annual Report and Financial Statements is signed off by the scheme's trustees.

An Annual Report and Accounts timetable is produced and agreed with auditors and trustees to produce signed accounts at a trustee meeting (or other agreed date if accounts are not being signed at a trustee meeting) within the statutory deadline. The difference to the timetable is managed by the lead pension plan accountant and delivery is monitored in conjunction with Secretary to trustees and auditors to ensure that the Report and Accounts are audited and signed by the due date. An accounts status spreadsheet is maintained for each client and the various stages of completion are signed by the preparer and the reviewer.	
Control Activity	**Auditor Testing and Results**
6.2.1: Annually, scheme accounts are prepared by the Accounts Team. The preparer, a member of the accounts team inputs the trial balance and member data into a statutory compliant Annual Report and Financial Statements template document. The draft document is reviewed and signed off by the preparer and the reviewer, another member of the accounts team, prior to audit by the scheme's external auditors.	6.2.1: For a sample of schemes, obtained the scheme accounts and confirmed these had been prepared by the accounts team. Confirm the draft document is reviewed and signed off by a preparer and an independent reviewer, prior to issue. No exceptions noted.

7 Information Technology - Restricting access to systems and data 7.1 Physical access to in-scope systems is restricted to authorised individuals.	
Process Description Each Hymans Robertson office has a controlled entry system and a staffed reception desk to monitor visitor movements.	
Control Activity	**Auditor Testing and Results**
7.1.1: Access to each HRLLP office is controlled by an electronic entry management system and a staffed reception desk.	7.1.1: Observed the physical access controls on-site and noted that access was restricted through a controlled entry system and a manned entry desk. No exceptions noted.

Process Description At each office, end user computing, printing and conferencing equipment is maintained in secure areas, only accessible to authorised staff. IT infrastructure equipment including servers, routers and emergency standby facilities are located within locked restricted areas only accessible by authorised IT personnel, or nominated individuals (e.g. Facilities Managers) A visitor requiring access to any restricted area, for example an engineer, is supervised by IT operational staff.	
Control Activity	**Auditor Testing and Results**
7.1.2: Access to end user computing / printing / conferencing equipment, is maintained in secure areas, restricted to authorised staff / visitors only. IT infrastructure equipment including servers, routers and emergency standby facilities is located within locked rooms.	7.1.2: Observed the physical access controls on-site and noted that computer equipment was maintained in a secure area with restricted access to authorised personnel only. Further noted that IT equipment, including servers, routers and emergency standby facilities, was located inside locked rooms. No exceptions noted.

Process Description Gas suppressants, in the event of a fire have been installed in accordance with Health and Safety requirements where the design and construction of office accommodation permits.	
Control Activity	**Auditor Testing and Results**
7.1.3: Gas suppressants have been installed in accordance with Health and Safety requirements where the design and construction of office accommodation permits.	7.1.3: Observed the physical access controls on-site and noted that gas suppressants have been installed in accordance with Health and Safety requirements where the design and construction of office accommodation permits. No exceptions noted.

Process Description Equipment is accessible only to those members of staff who require operational access and who are suitably authorised.	
Control Activity	**Auditor Testing and Results**
7.1.4: Equipment is accessible only to those members of staff who require operational access and who are suitably authorised.	7.1.4: Observed the physical access controls on-site and noted that physical access to the IT infrastructure is restricted to authorised individuals. Inspected the IT Operations Server Room Policy Handbook and noted that this was updated on a at least an annual basis (with the dates of revision documented) and contained a list of personnel authorised to access server rooms. No exceptions noted.

Process Description We have twin main power and back-up supplies to all our critical systems. Local area and wide area devices are also duplicated. All PCs and laptops are subject to a standard 'in-house' build and desktop format with enforced branding. Regular hardware and software audits are performed on all PCs to ensure compliance with internal IT policies. All staff sign up to our internal Information Security Policies as part of their employment contracts. For remote working, we have an 'acceptable use' policy, which covers the use of devices for remote working.	
Control Activity	**Auditor Testing and Results**
7.1.5: Staff sign up to our internal Information Security Policies as part of their employment contracts.	7.1.5: Inspected the Employee Handbook and noted that contractual adherence to Information Security policy is applied to all staff via this Handbook. Copies of the applicable IT policies are available to all staff via a central intranet site, which was observed via screen-sharing. No exceptions noted.

7.2 Logical access to in-scope systems and data, is restricted to authorised individuals in accordance with job roles and/or business requirements.
Process Description At Hymans we have a joiners/leavers/movers policy which prompts the review of users access and rights. Every new employee undertakes the following: • Information security induction.

- Compulsory information security and data protection training and are re-tested annually.
- Reads and signs that they will adhere to our information security policies once a year in our annual declaration.

At Hymans we employ role-based authentication where employees are only given access rights to data/areas necessary for their job role. Access specific groups are configured and comprised of specific user groups based on roles. The membership of these groups are emailed to business owners to review on a regular basis.

Privileged (local administrative) user access is restricted to those individuals with specific technical / or application requirement in line with their role or responsibilities. This is reviewed by the IT Leadership Team monthly.

Regular reporting is undertaken to document user access rights, this is sent to nominated representatives of Business Units to check users have the correct level of access to data relevant to their job role.

IT Personnel have elevated administrative rights on our systems and networks specific to their role.

Enforced changes to passwords occur at periodic intervals in accordance with network and application settings.

Control Activity	Auditor Testing and Results
7.2.1: New user access is established by a new starter form which must be authorised by the user's line manager and Human Resources.	7.2.1: For a sample of new starters, inspected the ticket and record maintained, and noted that a member of HR and their line manager had marked their approval on the electronic form. No exceptions noted.

Control Activity	Auditor Testing and Results
7.2.2: User accounts for staff that leave are closed by the IT team following submission of a leaver form which is authorised by the appropriate line manager.	7.2.2: For a sample of leavers, inspected the records maintained and noted that IT access had been revoked following appropriately authorised notification. Reconciled the population of leavers against the active user population and noted that no leavers had active user accounts. No exceptions noted.

Control Activity	Auditor Testing and Results
7.2.3: A monthly reconciliation of leavers is completed between the Human Resource records and the central IT records, ensuring that any discrepancies are investigated.	7.2.3: Inspected the leaver records and noted that completion of the monthly reconciliation had been recorded for all months within the in-scope period. No exceptions noted.

Control Activity	Auditor Testing and Results
7.2.4: An automated quarterly report is run showing user access rights. This is sent to Head of TPA and TPA Governance and Change Lead to review and check that users have the correct level of access to systems relevant to their job role. Once reviewed access that requires alteration is requested and actioned.	7.2.4: For a sample of quarters, the automated report was obtained along with the evidence of the Head of TPA and TPA Governance and Change Lead review. Where access changes were required, access change requests were raised and actioned through the IT service desk. No exceptions noted.

Control Activity	Auditor Testing and Results
7.2.5: Enforced changes to passwords occur at periodic intervals in accordance with network and application settings.	7.2.5: Inspected the configuration of the network password policy implemented and noted that it enforced periodic password changes via a configured maximum password age setting. No exceptions noted.

7.3 Client and third-party access to In-scope systems and data is restricted and/or monitored
Process Description Clients do not have access to our in-scope systems and data unless they have elected to have PRISM in their service order and will therefore have access to the employer portal in PRISM. Our secure digital access portal, PRISM offers our clients and pension scheme members a fully online, self-service option to manage their pension 24/7. The current release of PRISM is for member's only, however in Q3 of 2022 we will be launching the Employer Hub. The Employer Hub will allow Trustees and Employers to run real-time reports, such as SLA reports and membership statistics, and view administration reports online. The information available to users of the Employer Hub will be controlled by security settings based on user role profiles and also by UPM Client/Company reference, i.e., users who are not entitled to see any member data will only be able to view anonymous information, restricted to the UPM Client/Company reference that they have been assigned to. The ability to create new Employer/Trustee Users will be restricted to Super Users within our Administration teams. It is the responsibility of the Operations Leader to assign Super User status to individual team members. Employer Hub User Security Role profiles will be restricted as follows: • Administration – Users can run and view anonymised reports. • Read Only – Users can run and view reports and view member information. • Super User - Users can run and view reports and view member information and start processes in the admin teamwork tray Plans are in place for all clients to be transferred to PRISM over the course of the year with any new clients onboarded automatically going LIVE in PRISM and not pensionsWeb. Segregation of incompatible duties is enforced by user profiles and processing tasks within the pension's administration, pension payroll, cash management and systems maintenance operations. The set-up to access a network and an application is segregated and is granted to users in accordance with

their job responsibilities. Access to the network is controlled through individual usernames and passwords.	
Control Activity	**Auditor Testing and Results**
7.3.1: Access to the network and applications is segregated and is granted to users in accordance with their job responsibilities. Access to the HRLLP network is controlled through individual usernames and passwords.	7.3.1: Inspected the password configuration enforced and noted that accounts are restricted by usernames and passwords. Inspected the role profiles allocated to users within the UPM system and noted that access to functions within the system was restricted based on job role. No exceptions noted.

8 Providing integrity and resilience to the information processing environment 8.1 Scheduling and internal processing of data is complete, accurate and within agreed timescales. 8.2 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 transmissions of financial data including pension payroll and electronic banking use secure encryption algorithms and smart card technology. Data transmitted through e-mail is encrypted or, where preferred by our clients, using password protection.	
Control Activity	**Auditor Testing and Results**
8.1.1 & 8.2.1: Data transmissions of financial data including pension payroll and electronic banking use secure encryption algorithms and smart card technology. All data transmitted through email is at minimum protected by encryption.	8.1.1 & 8.2.1: Observed configuration settings showing that data transmissions are encrypted in-line with industry standards, including encryption via VPN. This is covered by an organisational 'Data Transfer and Encryption Policy'. Further observed and inspected evidence of the configuration of email protection and noted that both inbound and outbound emails were automatically scanned and required encryption, including checks for Data Loss Prevention.

Process Description BACS Bureau facilities are used to process pension payroll payments. This is accessed through internet-based software by authorised individuals who have been set up as either Approvers or Submitters. Each transmission needs two individuals to approve and submit it using passwords and PIN numbers. Smart cards have been issued to be used in a disaster recovery situation.	
Control Activity	**Auditor Testing and Results**
8.1.2 & 8.2.2: The BACs Bureau facility is accessed through internet-based software by authorised individuals who have been set up as either Approvers or Submitters.	8.1.2 & 8.2.2: Through observation, confirmed that the BACS Bureau facility is accessed through internet-based software and that this is limited to authorised individuals. No exceptions noted.

Process Description

Electronic banking transmissions are made through secure modem links with our relationship bank. A restricted list of authorised users only can affect electronic payments and transmissions.

Transaction data transmission confirmation with payment counterparties is evidenced as follows: electronic transmission of a payment with our relationship bank generates a transmission confirmation document; BACS confirmation takes the form of a transmission report and processing confirmation from BACSTEL-IP the day before the processing date.

Control Activity	Auditor Testing and Results
8.1.3 & 8.2.3: A restricted list of authorised users only can affect electronic payments and transmissions. The transmission confirmation document, in the form of a transmission report, is generated and processing confirmation from BACSTEL-IP the day before the processing date.	8.1.3 & 8.2.3: Confirmed authorised list of users in place to affect electronic payments and transmissions. Through observation, confirmed that a transmission confirmation report is generated when a BACS payment is made from BACSTEL-IP the day before processing date. No exceptions noted.

8.3 Network perimeter security devices are installed, and changes are tested and approved.

Process Description

A dedicated private circuit National Ethernet Wide Area Network (WAN) connecting our offices, with a private MPLS (Multi-protocol Label Switching) circuit links all four offices and acts as a back-up link between offices for fault tolerance.

All internet facing perimeter networks are protected by industry standard firewalls that employ an IPS engine to prevent malicious activity which support a dedicated WAN and MPLS circuit setup between offices.

There are formalised policies in place, including a Rule Base Policy and Firewall Management Policy, which are used to govern the management of the firewall and its rule base.

Any changes to the firewall or rule base would follow the standard change management process. This includes the documentation of changes in the internal IT Service Management solution, approval via Change Advisory Boards and testing where appropriate, with approval, testing and implementation notes retained in the Service Desk ticket.

Control Activity	Auditor Testing and Results
8.3.1: Industry standard firewalls with Intrusion Protection Systems (IPS) are installed at the network perimeter, these support a dedicated WAN and MPLS circuit setup between offices. Firewall events (e.g., attempted hacking, logins at unusual hours) are monitored and managed by our dedicated Networks and Security team. There are formalised policy documents, including a Rule Base Policy and Firewall Management Policy,	8.3.1: Observed the configuration of the firewall and noted that these were in place and monitored by the CheckPoint application. Further observed that policies were in place covering the usage of firewalls, and noted from inspection that changes were logged as tickets. For a sample of changes to the firewall, inspected the associated ticket and noted that it had been raised, authorised, tested, and actioned appropriately.

which are used to govern the management of the firewall and its rule base. Firewall changes are tested and approved before implementation, managed within service desk solution.	No exceptions noted.

Process Description

An annual Penetration test (pen test) is run on external facing sites and systems by a third party, in addition all new systems are tested before going live. The results of these reviews and tests are distributed internally to the appropriate management and client teams. These include vulnerability scanning. As part of the test, known vulnerabilities are checked that are specific to vendor, platform, and version. Ad hoc penetration test area is also conducted on new applications before being released to live environments. The last annual penetration test was conducted in October 2022.

The results of the tests are distributed internally to the appropriate management and applications owners to review and agree an action plan to remediate any issues found. Depending in the severity of the issue the remediations are planned into work schedules over the course of following 12 months up to the date of the next annual pen test. High priority issues were addressed immediately.

Control Activity	**Auditor Testing and Results**
8.3.2: An annual Penetration test is run on external facing sites, systems by a third party and new systems before going live. A report detailing the results of the tests are distributed internally to the appropriate management and applications owners to review and agree an action plan to remediate any issues found. Depending in the severity of the issue the remediations are planned into work schedules over the course of following 12 months up to the date of the next annual pen test. High priority issues are addressed immediately.	8.3.2: Inspected a confirmation of penetration testing completion provided by the third-party penetration testing service providers and noted that a penetration test was performed by the third party during the in-scope period. Inspected an email demonstrating that the penetration testing report had been circulated to all applicable personnel. Inspected a report summary produced by Hymans management for their clients and noted that the number of findings and their criticality were recorded. Further noted that no Critical or High rated findings had been identified. Moreover, noted that the summary contained details of the plans for remediation of the identified findings, and that these would be worked into the change management schedule during 2023. No exceptions noted.

8.4 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 The threat from malicious electronic attack is mitigated by the installation of industry standard firewalls, multi-layered anti-virus solutions and vulnerability management solutions. The anti-virus / malware solutions we have installed scan any file prior to opening. Should any virus or malware be detected, automated actions are undertaken to quarantine files and an incident is logged via our internal service desk solution which is accessible by IT Operations. Follow-up action is taken.	
Control Activity	**Auditor Testing and Results**
8.4.1 The threat from malicious electronic attack is mitigated by the installation of firewalls and anti-virus software.	8.4.1: Inspected the configuration of the anti-virus solution and noted that an anti-virus solution was in place, which had both anti-malware and anti-phishing protection enabled, and notified IT upon detecting positives. Further inspected the email security scanning application and noted that anti-malware scanning was configured for inbound emails, with automatic notification and quarantine. See 8.2.1 for firewall management test results. No exceptions noted.

8.5 Data received from external parties is scanned for known vulnerabilities, any compromised data is quarantined, and definitions of threats are periodically updated.	
Process Description Prior to any email entering a user's inbox, messages are scanned for known vulnerabilities by multi-layered security solutions. Any hyperlinks and attached are scanned, as well as the email itself for viruses, malware, and the reputation of the IP address. Anti-virus software will scan any file prior to opening and any virus or malware detected will be automatically reported to Service Desk for resolution. On all laptops and servers, multiple anti-virus solutions are in place which together act to scan and/or analyse at varying levels and frequencies for known threats. Any identified compromised data is automatically quarantined, and all products automatically update for new definitions and updates, as required. Removable devices, which may be used to transfer data, are blocked by default, with exceptions requiring approval and autoplay functionality disabled.	
Control Activity	**Auditor Testing and Results**
8.5.1: Prior to any email entering a user's inbox, messages are scanned for known vulnerabilities by multi-layered security solutions. Any hyperlinks and attached are scanned, as well as the email itself for viruses, malware, and the reputation of the IP address. Anti-virus software scans any file prior to opening.	8.5.1: Inspected the configuration of the anti-virus solution and noted that an anti-virus solution was in place. Inspected the Data Loss Prevention (DLP) in place for emails and noted that emails were scanned by the tool, including any attachments.

Any virus or malware detected is automatically quarantined and reported to the IT Service Desk for resolution. Removable devices are blocked by default, with autoplay disabled for any exceptions to this rule.	For the anti-virus solution, email scanning solution, and the DLP solution, noted from inspection that in all cases IT personnel were automatically notified should any suspicious activity be detected. Inspected the configuration for the blocking of USB devices, and noted that phone/tablet operating systems, still images, USB CD DVD RW drives, USB drives, VMWare USB Passthroughs, and Windows Portable Devices were blocked, with Device Control enabled. Further noted that the Workstation Security Settings were configured to disable autoplay for all drives. No exceptions noted.

9 Maintaining and developing systems hardware and software

9.1 Development and implementation of both in house and third party in-scope systems are authorised, tested, and approved.

Process Description

Network applications across Hymans Robertson are developed and maintained through operational controls and test environments before release to live operation and use.

Software and hardware support and maintenance is provided by the IT support team and all requests for support are recorded, monitored, and controlled through an internal on-line help desk and logging facility.

High level network and software solutions are analysed, reviewed, tested, and released through internally designed project management controls.

PRISM, our secure digital access portal, allows members a fully online, self-service option to manage their pension 24/7. Placing Digital at the heart of our administration and client services, PRISM has been developed and tested with extensive input and feedback from real life scheme members, to ensure it provides a seamless online user-experience. It also brings a fresh, modern look, is intuitive to use and adaptive to any mobile device type, allowing members to access in the way they choose.

Quality Assurance and User Acceptance Tests are performed within dedicated non-production environments, using anonymous datasets. Development & release protocols are followed to ensure that each development requirement is documented as a work item, with acceptance criteria detailed within, which is followed and recorded as pass/fail. Evidence of tests is attached, any failed steps are cycled back through the development process, and the process repeats. Once acceptance criteria is met, the work item is approved and released by authorised individuals.

Only authorised individuals have access to live data or applications.

Control Activity	Auditor Testing and Results
9.1.1: Testing on the code is carried out in a dedicated test environment. Testing against each work item is recorded on UPM with test steps being passed or failed and screenshot and text evidence attached to the system; any failed step is investigated. Once testing is complete code is approved to move to UAT, or Live, environment by three individuals who are not involved in testing.	9.1.1: For a sample of deployments, inspected the documentation retained, and noted that: the deployment had mapped its acceptance criteria to its test plan; each test had been documented; test evidence had been retained; failed tests had been followed-up and reperformed; and the deployment had been implemented by a separate individual to the developer and tester following authorisation, as enforced by the system. No exceptions noted.

Process Description

Development, maintenance, and upgrades to the UPM administration system are controlled through the TPA systems support team. All changes to the UPM software are analysed and tested in secure database environments and approved before release to the live database.

Control Activity	Auditor Testing and Results
9.1.2: Development, maintenance, and upgrades to the UPM administration system are controlled	9.1.2: For a sample of UPM application releases, inspected the documentation retained, and noted

through the TPA systems support team. All changes to the UPM software are analysed and tested in secure database environments and approved before release to the live database.	that: the release had mapped its acceptance criteria to its test plan; each test had been documented; test evidence had been retained; failed tests had been followed-up and reperformed; and the release had been authorised prior to implementation into the live environment. No exceptions noted.

Process Description

There are internal processes in place for recording and controlling all changes including improved functionality through fixes and upgrades released by the UPM software provider (Civica plc). These changes are tested initially in a segregated environment prior to being released to the test and live platforms.

Client specific and internal software developments are undertaken by the TPA systems support team and are released to the test environment for user testing and sign-off prior to release onto the live platform.

Control Activity	**Auditor Testing and Results**
9.1.3: Client specific and internal software developments are undertaken by the TPA systems support team and are released to the test environment for user testing and sign-off prior to release onto the live platform.	9.1.3: For a sample of client specific development requests, inspected the documentation retained, and noted that: the deployment had mapped its acceptance criteria to its test plan; each test had been documented; test evidence had been retained; failed tests had been followed-up and reperformed; and the deployment had been implemented by a separate individual to the developer and tester following authorisation, as enforced by the system. No exceptions noted.

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

Process Description

Data migration or modification is subject to testing and validation which is completed by both the TPA systems support team and the administration teams. For example, when taking on a new client as noted on the new client installation checklist.

Control total and validation tests are applied at a high level by the systems support team for any bulk data migration or modification exercises, for example when taking on a new client. Validation tests are reconciled back to source data.

All data migration and bulk change work is completed within a test environment and subject to TPA system team and user acceptance testing. Once authorised, data is transferred to the live operating database and again subject to validation and testing before signing off by the receiving administration teams.

Day to day operational data changes, data loads and maintenance is performed by the administration teams following the embedded workflow processes within the UPM system.

Control Activity	Auditor Testing and Results
9.2.1: Data migration or modification is subject to testing and validation which is completed by both the TPA systems support team and the administration teams when taking on a new client.	9.2.1: For a sample of data migrations during the in-scope period, inspected the retained documentation, and noted that the migration had been tested and validated by both the TPA systems support team and the administration team. No exceptions noted.

9.3 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 A DevOps approach is used for change management, supported by Change Management Process documents which identify the authorisation, testing and approval approach for each type of change. Administrative permissions for changes to our systems are restricted to support staff. Software is typically deployed centrally via MECM. Change control processes are in place for configuration changes, including software installations for servers. Patch management is centrally controlled on a monthly schedule. Critical and security updates for both servers and workstations are applied in line with industry best practice. Out of band patching is conducted as and when required.	
Control Activity	**Auditor Testing and Results**
9.3.1: Change management processes are in place for all changes covering authorisation, testing, approvals, and implementations. This applies to normal and emergency changes. Administrative permissions for changes are restricted to support staff. Changes are downloaded and deployed via WSUS and managed via MECM (software).	9.3.1: Enquired of management and were informed that the TPA System team log changes in the Service Desk/Change solution, and that a change management process, including a Change Advisory Board (CAB), is in place for all changes. Restriction of permissions based on role has been tested in 7.3.1. Observed the mechanism for change deployment and noted that it is as described in the control wording. For a sample of changes, observed the record within the system and noted that it had followed the established change management process. No exceptions noted.

10 Recovering from processing interruptions

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

Process Description

A comprehensive business continuity plan has been designed to cover: the total denial of access to any office, the loss of the main business streams and support functions to include a pandemic.

Disaster recovery is the joint responsibility of the applications team and the IT Operations department. Disaster recovery is tested for critical applications on an annual basis. Hymans have a business continuity plan which is aligned with the ISO 22301, it consists of emergency response, crisis management and business recovery. The Business Continuity Manager is responsible for the plans and the plans are reviewed and approved annually.

Control Activity	Auditor Testing and Results
10.1.1: A comprehensive business continuity plan has been designed to cover: the total denial of access to any office, the loss of the main business streams and support functions to include a pandemic.	10.1.1: Inspected the Business Continuity Plan (BCP) and noted that a BCP was in place and took the form of an overarching Policy Pack which referred staff to more granular documentation, including packs with necessary contact information. Noted from inspection that these covered the total denial of access to any office, the loss of the main business streams, and support functions to include a pandemic. The BCP had been reviewed and updated during the in-scope period. No exceptions noted.

Process Description

When an incident has been identified, the Emergency Response Team is formed; the Emergency Response Co-Ordinator will in discussion with senior management, typically members of the Crisis Management Team, agree to invoke the Business Continuity Plan.

In the event of total denial of access to any office, Hymans Robertson has the capability for all staff to work from home. The IT infrastructure has been designed and constructed with high levels of resilience to ensure systems can be recovered at an alternative site and Hymans Robertson can operate independently from another office location.

There is the capability to immediately divert telephone lines to other offices to process calls. Each member of staff has access to the disaster recovery cards, which gives details of the disaster recovery office location and contact information. In addition, there is a text alert system for all staff and a separate disaster recovery website to keep staff informed.

The roles and responsibilities of the teams involved in the Business Continuity Plan are tested at each office location on a rolling basis using scenarios to exercise the different parts of the Plan, the latest exercise having taken place in March 2022.

Control Activity	Auditor Testing and Results
10.1.2: The roles and responsibilities of the teams involved in the Business Continuity Plan are tested	10.1.2: Inspected the BCP Policy Pack and noted that it listed BCM exercises as part of its ISO22301

at each office location on a rolling basis using scenarios to exercise the different parts of the Plan.	Compliance schedule. The pack further documented that exercise documentation was retained internally within SharePoint. Inspected the report for the most recent BCP exercise undertaken and noted that it was performed on 30 March 2022. The report included documentation of the feedback, lessons learned, and the agreed resulting actions, with updates against these provided. Noted that these had all been subsequently completed and initialled by the action owner. No exceptions noted.

Process Description IT recovery tests are undertaken annually. We use cloud-based recovery solutions, from which file restoration is undertaken, for our data and servers. Recovery tests have been carried out in 2022.	
Control Activity	**Auditor Testing and Results**
10.1.3: IT recovery tests are undertaken annually. We use cloud-based recovery solutions for our data and servers.	10.1.3: Inspected the documentation around the latest failover test and noted that this was a failover of the selected server from on-premises to a cloud recovery solution. Inspected the configuration of the cloud recovery solution and noted that all Virtual Machines (VMs) which were not undergoing decommission had been successfully replicated, and the last failover was within the previous 180 days. No exceptions noted.

10.2 In-scope systems and data are backed up and tested such that they can be restored completely and within agreed timescales.	
Process Description Data is backed up using a variety of methods: SAN to SAN and Disk to Disk and Disk to Cloud. SAN to SAN replication is carried out between our Glasgow and London data centres daily. Snapshots are performed every 8 hours with every third snapshot (00:00) retained for 7 days and every seventh daily snapshot (00:00) retained for four weeks. These snapshots are used for DR purposes. Disk to Disk backups are conducted locally for short term data retention and restores. File and Application servers have two recovery points performed daily which are retained for 28 days. Application aware SQL backups with transactional logging are performed every 30 minutes and held for 28 days. Disk to Cloud backups are carried out once a month for long term data retention into the Azure cloud which are retained for 12 months.	
Control Activity	**Auditor Testing and Results**
10.2.1: SAN to SAN replication is carried out between our Glasgow and London data centres	10.2.1: Enquired of management and were informed that IT personnel receive emails alerting on the

daily in line with the above process. Disk to Cloud backups are carried out once a month for long term data retention into the Azure cloud which are retained for 12 months.	current status of replications, which is also available within the solution's dashboard. Inspected the configuration of the SAN to SAN replication and noted that mirror replications are taken asynchronously according to a pre-defined transfer schedule. The Transfer Status was visible within this dashboard configuration screen. Inspected the backup policy and retention configuration for backups to the Azure cloud and noted that backups were configured for a daily basis and kept for 31 days, with the backup taken on the last Friday of each month retained for 12 months as a monthly backup. No exceptions noted.

Process Description For both daily and monthly back-ups, the IT Service Desk carry out daily test data restores. Failed back-up jobs are investigated and re-run at the earliest possible opportunity. Back-up jobs have a built in verify which is run to check and verify the integrity.	
Control Activity	**Auditor Testing and Results**
10.2.2: Back-up activity for key systems is undertaken to comply with a daily and weekly schedule.	10.2.2: Observed the backup schedules confirming that daily and weekly backups are configured in accordance with the control description. No exceptions noted.

10.3 Problems and incidents relating to in-scope systems are identified and resolved within agreed timescales	
Process Description All production hardware is implemented in a highly available configuration. Servers have fully resilient power and cooling configurations. Network infrastructure has been designed with high availability in mind, and dual firewalls, switches, network connections are in place for all systems. For all applicable systems providers, there are Contracts, incorporating SLAs, in place providing support response times to agreed timescales. We have a “Security Incident Reporting Policy” that covers network intrusion incidents. We receive alerting on security threats and vulnerabilities from platforms and systems employed to detect and manage security incidents, as well as threat intelligence from trusted partners. We employ solutions to centrally manage security incident and events (SIEM) and well as to monitor operational availability of infrastructure.	
Control Activity	**Auditor Testing and Results**
10.3.1: A Security Incident Reporting Policy is used to govern processes around network intrusion incidents; this is supported by automated alerts	10.3.1: Inspected the repository of Information Security policies at Hymans and noted that an Information Security Incident Reporting Policy is in

from installed systems and event management tools to IT for monitoring and resolution. Technical support contracts with Service Level Agreements (SLA's) are in place with key system providers.	place. Supplier response times and further policy and procedural documentation form part of the Business Continuity and Disaster Recovery testing. For a sample of events, inspected the records retained and observed the alerting mechanisms, and noted that the events were alerted, logged, and resolved. No exceptions noted.

10.4 The physical IT equipment is maintained in a controlled environment.	
Process Description At Hymans we have hybrid hosting consisting of an in-house private infrastructure in our own data centres in the UK utilising virtual servers deployed on dedicated hypervisor infrastructure, we also have a cloud computing policy and host data in Microsoft Azure, a multi-tenant public cloud. Depending on the services consumed by clients, data can be in held a combination of our in-house and/or Azure data centres. Services exclusively hosted on our in-house data centre in the UK are backed up to Azure and held in the Azure UK data centre. IT equipment including servers, routers and emergency standby facilities is located within locked rooms.	
Control Activity	**Auditor Testing and Results**
10.4.1: IT equipment including servers, routers and emergency standby facilities is located within locked rooms.	10.4.1: Observed the physical access controls on-site and noted that computer equipment was maintained in a secure area and noted that IT equipment, including servers, routers, and emergency standby facilities, was located inside locked rooms. No exceptions noted.

10 Club Vita - Information Security

11 Restricting access to systems and data 11.1 Logical access to Club Vita computer systems, programs, master data, transaction data and parameters, including access by administrators to applications, databases, systems, and networks, is restricted to authorised individuals within the Club Vita operations team in accordance with the Club Vita System Access Control Policy
Process Description Logical access will be granted to network and applications by IT operations and Club Vita IT applications team in accordance with the System Access Control Policy. New user access is established by the Club Vita IT applications team following submission of an Electronic Data Security Form which must be authorised by relevant authorisers as specified in the System Access Control Policy.

Control Activity	**Auditor Testing and Results**
11.1.1: New user access is established by the Club Vita IT applications team following submission of an Electronic Data Security Form which must be authorised by relevant authorisers as specified in the System Access Control Policy.	11.1.1: For a sample of starters, inspected the electronic security form retained, and noted that it had been completed and that appropriate authorisation for the access had been recorded. No exceptions noted.

Process Description User accounts for staff that leave are closed by the IT team following submission of a leaver form which is authorised by the appropriate line manager.

Control Activity	**Auditor Testing and Results**
11.1.2: User accounts for staff that leave are closed by the IT team following submission of a leaver form which is authorised by the appropriate line manager to ensure that access has been removed.	11.1.2: Informed by management that staff who leave the organisation completely follow the standard Hymans leaver control tested within 7.2.2. However, a ticket is completed by Club Vita management when a user moves internally and no longer requires Club Vita access. For a sample of these movers, inspected the form for access revocation and noted that it had been completed and authorised. No exceptions noted.

Process Description A quarterly report is produced and reviewed by the Club Vita operations team to ensure only authorised Hymans Robertson and Club Vita UK users can access all Club Vita specific systems, networks, and data and at the appropriate level of access.	
Control Activity	**Auditor Testing and Results**
11.1.3: A quarterly report is produced and reviewed by the Club Vita operations team to ensure only authorised Hymans Robertson users can access all Club Vita specific systems, networks, and data and at the appropriate level of access.	11.1.3: For a sample of quarters, inspected the access report produced and noted that management had actively commented against any changes in access. Inspected the associated review checklist and noted that the review had been appropriately authorised. No exceptions noted.

Process Description Logical access by privileged users is restricted to those individuals with specific technical network and application job responsibilities and their requirement to resolve issues arising.	
Control Activity	**Auditor Testing and Results**
11.1.4: Logical access by privileged users is restricted to those individuals with specific technical network and application job responsibilities.	11.1.4: Inspected the current and historical user access level reports. Noted that access was restricted based on role using separate levels. Noted that the highest level of access was limited to staff with (or management of) technical network and application-specific responsibilities. No exceptions noted.

Process Description Enforced changes to passwords occur at periodic intervals in accordance with network and application settings.	
Control Activity	**Auditor Testing and Results**
11.1.5: Enforced changes to passwords occur at periodic intervals in accordance with network and application settings.	11.1.5: Inspected the password policy configured within the domain for users and noted that passwords for both regular and administrative users would forcibly expire after 90 days. No exceptions noted.

11.2 Logical Client Web Access to Club Vita master data, transaction data and reports is restricted to authorised individuals at Clients in line with the Club Vita Client Setup Policy.	
Process Description Logical access will be granted to network and data in accordance with the authorisation by the Club Vita operations and Club Vita IT applications teams. New user access is established by the IT applications team following submission of a Club Vita Member Site Login Request from the Club Vita operations team. The Club Vita Operations team approve a member site login request before it goes live on the Hymans IT service desk, called SAW.	
Control Activity	**Auditor Testing and Results**
11.2.1 New user access is established by the IT applications team following submission of a Club Vita Member Site Login Request from the Club Vita operations team.	11.2.1: For a sample of login requests, inspected the request raised and completed forms. Noted that access was requested via the raising of a service desk ticket and completion of a request form by the Club Vita Operations Team and actioned accordingly by the IT applications team. No exceptions noted.

Process Description Client data is uploaded to the website over a secure socket layer (SSL). Clients may load and view data and reports securely through the SSL but not modify or delete reports. Clients may only view and load data to their own client specific areas of the website via the SSL. A quarterly report of individual client users, roles and access levels is independently reviewed by the Club Vita operations team each quarter.	
Control Activity	**Auditor Testing and Results**
11.2.2: A quarterly report of individual client users, roles and access levels is independently reviewed by the Club Vita operations team each quarter.	11.2.2: For a sample of quarters, inspected the quarterly report produced, and noted that it had been reviewed and signed-off appropriately. No exceptions noted.

Appendix

Service Auditor's Letter of Engagement

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/AAF01-20/2022.23
Your ref:

8 March 2023

Strictly Private & Confidential

The Partners
Hymans Robertson LLP
One London Wall
London
EC2Y 5EA

To the Partners of Hymans Robertson 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 Technical Release AAF 01/20 issued by the Institute of Chartered Accountants in England and Wales ('Service' or 'Services') and International Standard on Assurance Engagements ("ISAE") 3402 – Assurance Reports on Controls at a Service and our respective areas of responsibility. Our services are provided in accordance with the attached Terms and Conditions of Business dated December 2021.

RESPONSIBILITIES OF SENIOR MANAGEMENT

Those charged with governance ('Senior Management') of Hymans Robertson 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. Senior Management's responsibilities are and shall include:

- acceptance of responsibility for internal controls;
- evaluation of the effectiveness of the Service Organisation's Control Activities using suitable Control Objectives;
- supporting their evaluation with sufficient evidence, including documentation; and
- providing a written report ('Management Statement') of the effectiveness of the Service Organisation's internal controls for the relevant 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 and ISAE 3402 but they may add to these to the extent that this is considered appropriate in order to meet User Entities' expectations.

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 at Birmingham, Edinburgh, Glasgow and London as described in the Management Statement and report this to Senior Management.

SCOPE OF THE SERVICE AUDITOR'S WORK

We conduct our work in accordance with the procedures set out in AAF 01/20 and ISAE 3402. 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 and ISAE 3402.

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, as amended.

We may seek written representations from Senior Management in relation to matters on which independent corroboration is not available. We shall seek confirmation from Senior Management that any significant matters of which we should be aware have been brought to our attention.

PROFESSIONAL ETHICS

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

INHERENT LIMITATIONS

Senior Management acknowledge that Control Activities designed to address specified Control Objectives are subject to inherent limitations and, accordingly, errors or irregularities may occur and not be detected. Control Activities cannot guarantee protection against fraudulent collusion especially on the part of those holding positions of authority or trust. Furthermore, the opinion set out in the Service 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 Senior Management of the Service Organisation, and solely for the purpose of reporting on the internal controls of the Service Organisation, in accordance with these terms of our engagement.

Our work will be undertaken so that we might report to Senior Management those matters that we have agreed to state to them in the Service Auditor's Report and for no other purpose.

The Service Auditor's Report will be issued on the basis that it must not be recited or referred to or disclosed, in whole or in part, in any other document or to any other party, without the express prior written permission of the Service Auditor. We permit the disclosure of the Service Auditor's Report, in full only, to existing and prospective User Entities of the Service Organisation using the Service Organisation's pension administration services and related information technology ('User Entities'), and to the auditors of such User Entities, to enable User Entities and their auditors to verify that the Service Auditor's Report has been commissioned by Senior Management of the Service Organisation and issued in connection with the internal controls of the Service Organisation without assuming or accepting any responsibility or liability to them on our part. 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 Senior Management as a body and the Service Organisation for our work, for the Service Auditor's Report or for the opinions we will have formed.

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:

TERM AND BREAK CLAUSE

1. The engagement shall endure for an initial term of three (3) years (the "Initial Term") to commence on the date of signing of this letter by the Service Organisation (the "Commencement Date") and shall continue until:

    (a) the third anniversary of the Commencement Date or

    (b) any date within the Initial Term upon which it is terminated by either party in accordance with clause 1.5 of the Terms and Conditions of Business;.

2. Notwithstanding the foregoing, the Service Organisation may terminate this engagement, by giving written notice to us to terminate the engagement at least thirty (30) days before the second anniversary of the Commencement Date, in which case the engagement shall terminate on the second anniversary of the Commencement Date.

CLAUSES TO BE ADDED, REMOVED OR AMENDED

1. The following clauses shall be added in section 5:

'5.13 To the fullest extent permitted by law, the Service Organisation agrees to indemnify and hold harmless RSM UK Risk Assurance Services LLP and its partners and staff against all actions, proceedings and claims brought or threatened against RSM UK Risk Assurance Services LLP or against any of its partners and staff by any persons other than the Senior Management as a body and the Service Organisation, and all loss, damage and expense (including legal expenses) relating thereto, where any such action, proceeding or claim in any way relates to or concerns or is connected with any of RSM UK Risk Assurance Services LLP's work under this engagement letter. This indemnity is not subject to the exclusions and limitation of liability detailed in clauses 5.14 and 5.15'

'5.14 Nothing in the Engagement Letter shall operate to exclude or limit either party's liability for death or personal injury caused by its negligence or any other liability which cannot be excluded or limited under

applicable law. The Service Organisation shall not be liable to RSM UK Risk Assurance Services LLP and its partners and staff for any loss of profit, anticipated profits, revenues, anticipated savings or business opportunity, or for any indirect loss or consequential loss or damage.

5.15 Subject to clause 5.14, Service Organisation's total aggregate liability to RSM UK Risk Assurance Services LLP of whatever nature arising out of or in connection with the engagement and Engagement Letter (including as a result of breach of contract, negligence or any other tort, under statute or otherwise) in respect of all claims by you under or in connection with this engagement shall be limited to the amount of fees paid or payable under this engagement.

2. The following clause shall be added as a new Clause 10.5 as follows:

"We shall, upon your written demand at any time, (i) return all Information relating to your business, products, affairs and finances for the time being confidential to you (including copies) in all formats held; (ii) in the case of Information stored electronically, delete the Information from all electronic devices within the possession, custody or control of us, our affiliates or personnel, and on request provide you with written confirmation of the same. For the avoidance of doubt, nothing in this clause 10.5 shall require us to return or destroy any documents or materials containing or based on your Information that:

a) we are required to retain by applicable law or to satisfy the requirements of a regulatory authority or body of competent jurisdiction; or

b) we retain on our backup and disaster recovery systems to the extent that such return or destruction of Information would be commercially practicable."

3. The following clauses shall be amended:

a) The definition of "Engagement Letter" shall be amended to:

"The letter (including any side letter detailing the level of fees to be paid for Services rendered) that incorporates these Terms and Conditions of Business together with these Terms and Conditions of Business or as may be varied from time to time in accordance with clauses 1.3 and/or 2.1."

b) In the fifth line of Clause 8.1 after the words "(at our own expense") insert:

"subject to obtaining the prior written consent of the Service Organisation".

c) Clause 33.1 shall be amended by deleting the following words in the fifth line "the law of the country in the UK in which your engagement partner resides, as identified in the Engagement Letter, unless we agree with you that some other law will apply before the start of the Engagement Letter" and replacing them with "the laws of England and Wales".

4. Existing Clause 5.9 of the terms to be deleted and replaced with: 'Any claim must be formally commenced within two years after the party bringing the claim becomes aware of the facts which give rise to the action (and in any case subject to the applicable statutory limitations period).'.

5. The following Clauses shall be removed:

a) Clause 10.5.

b) Clause 10.6.

AGREEMENT OF TERMS

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

For the avoidance of doubt, the terms covered by the Engagement Letter shall take effect upon receipt by us of your written agreement to them, or upon commencement of the work to which they relate, whichever is the sooner.

Yours faithfully,

RSM UK Risk Assurance Services LLP

RSM UK Risk Assurance Services LLP

Encs. Terms and Conditions of Business dated December 2021

Contents noted and agreed for and on behalf of Hymans Robertson LLP

Signed *Shirley Brown* ……
AUTHORISED SIGNATORY

Date 17/03/23 ……

London | Birmingham | Glasgow | Edinburgh T 020 7082 6000 | www.hymans.co.uk