

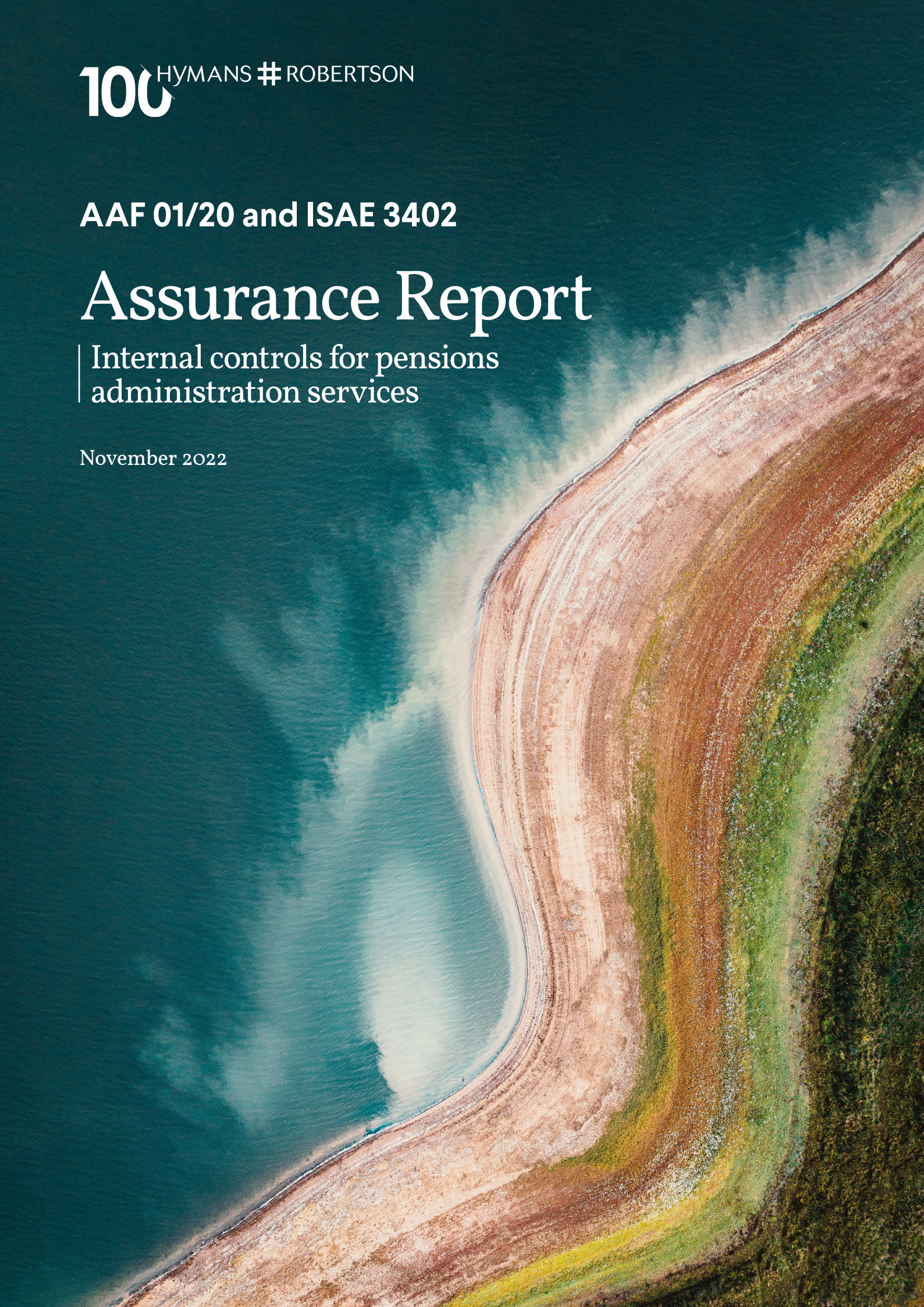
100 HYMANS # ROBERTSON

AAF 01/20 and ISAE 3402

Assurance Report

| Internal controls for pensions
administration services

November 2022



Contents

1	Executive Summary	1
2	Report of the Partners of Hymans Robertson LLP	4
3	Overview of Hymans Robertson LLP	5
4	Pensions administration business unit	7
5	Service auditor's assurance report on internal controls to the Partners of Hymans Robertson LLP	10
6	Summary of control objectives	12
	Pensions administration	12
	Information technology	13
	Club Vita - Information technology	14
7	Control objectives and control activities	15
	1. Accepting clients	15
	2. Authorising and processing transactions	19
	3. Maintaining financial and other records	25
	4. Safeguarding assets	31
	5. Managing and monitoring compliance and outsourcing	38
	6. Reporting to clients	44
	7. Restricting access to systems and data	46
	8. Providing integrity and resilience to the information processing environment	51
	9. Maintaining and developing systems hardware and software	57
	10. Recovering from processing interruptions	61
	11. Managing and monitoring compliance and outsourcing	67
	Club Vita - Information Security	68
	1. Restricting access to systems and data	68
	Appendix	72

1 Executive Summary

Introduction

Hymans Robertson LLP (“Hymans Robertson”) is a limited liability partnership providing pensions administration services since 1984.

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

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

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, welcomed the opportunity to have our administration procedures reviewed by external auditors, and have appointed Crowe U.K. LLP, our reporting accountants, to appraise the design and description of the controls within our administration business unit. Their report is set out in Section 6.

We have adopted the framework provided by the Audit and Assurance Faculty of the Institute of Chartered Accountants in England and Wales ‘Assurance Reports on internal controls of service organisations made available to third parties’ (AAF01/06) 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.

This report covers the controls in place and which were applied over the period 1 February 2021 to 31 January 2022, in accordance with the AAF 01/20 and ISAE 3402 framework.

We include a summary of the controls tested overleaf and are pleased that there have been no material failings in our control environment.

Summary of controls tested

Pensions administration

Control objectives	Number of Key Controls tested	Pages	Summary of results of testing
1. Accepting clients	3	15 - 18	1 exception
2. Authorising and processing transactions	8	19 - 24	No exceptions
3. Maintaining financial and other records	10	25 – 30	No exceptions
4.Safeguarding assets	17	31 - 38	No exceptions
5.Managing and monitoring compliance and outsourcing	10	38 - 43	No exceptions
6.Reporting to clients	4	44 - 46	No exceptions

Information technology

Control objectives	Number of Key Controls tested	Pages	Summary of results of testing
7. Restricting access to systems and data	12	46 - 51	1 exception
8. Providing integrity and resilience to the information processing environment	8	51 - 56	No exceptions
9. Maintaining and developing systems hardware and software	5	57 - 60	No exceptions
10. Recovering from processing interruptions	9	61 - 66	No exceptions
11.Managing and monitoring compliance and outsourcing	0	67	No exceptions

Club Vita

Control objectives	Number of Key Controls tested	Pages	Summary of results of testing
1. Restricting access to systems and data	8	68-71	No exceptions

Management response to exceptions identified

Pensions administration

Exception 1

Procedure

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.

Exception

For one client a signed-off checklist was not available. Ordinarily someone from the administration team would complete this and the project manager would perform the sign-off. In this particular case, the senior project manager was responsible for sharing the document, saving down all of the items received and checking that what was received was correct before marking each item as complete. This did not occur.

Management response

On this occasion, due process was not followed. The team have been reminded of the importance of ensuring that process is followed and correct sign-off is recorded. The senior project manager had daily catchups with all stakeholders and regular calls with the client. All actions were complete except for the checklist sign-off.

The missing checklist sign-off is shown as an exception in the report, impacting one control.

Exception 2

Procedure

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

Exception

For one sample out of nine, an individual, a contractor with a leave date of 31 December 2021, did not have his account disabled until 11 January 2022. The individual was in the process of re-negotiating his contract and when his contract was not renewed, this was not communicated to IT until 11 January 2022.

Management Response

This is not a scenario that occurs frequently; however, we have made teams aware of the importance of notifying I.T once a contract of employment is due to end and to confirm the end-date.

This has been noted as an exception in the report, impacting one control.

2 Report of the Partners of Hymans Robertson LLP

The partners are responsible for the identification of control objectives relating to clients' assets and related transactions in the provision of pensions administration services as well as the design, implementation and operation of the Control activities of Hymans Robertson to provide reasonable assurance that the control objectives are achieved.

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

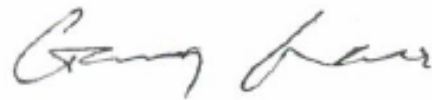
We have evaluated the effectiveness of our Control activities having regard to the Institute of Chartered Accountants in England & Wales Technical Release AAF 01/20 and the criteria for pensions administration set out therein.

We set out in this report a description of the relevant Control activities at our London, Glasgow and Birmingham offices together with the related control objectives which operated during the period 1 February 2021 to 31 January 2022 and confirm that:

- the report describes fairly the Control activities that relate to the control objectives referred to above which were in place during the year ended 31 January 2022;
- the Control activities described in Section 7 are suitably designed such that there is reasonable assurance that the specified control objectives would be achieved if the described Control activities were complied with satisfactorily; and
- the Control activities described were operating with sufficient effectiveness to provide reasonable assurance that the related control objectives were achieved during the period specified.

Details of our business structure, operating environment and the report of the reporting accountants, Crowe U.K. LLP, can be found in the following sections.

Signed on behalf of the Partners of Hymans Robertson LLP



Gary Evans

Head of Third Party Administration

November 2022



3 Overview of Hymans Robertson LLP

Established history and structure

Founded in 1921, we're one of the longest established independent firms of consultants and actuaries in the UK and are currently celebrating our centenary year. We are a limited liability partnership. Ownership lies with the partners who are fully involved in the day-to-day management of Hymans Robertson.

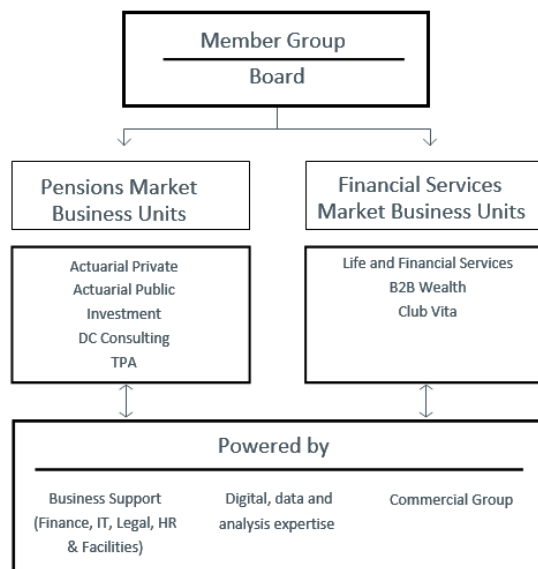
Specialising in advisory and management services to the occupational pensions market, in both private and public sectors, we provide all the core services such as:

- 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 1,000 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 five 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. This is a change that came into effect from April 2019 where before it was a practice and segment organisation structure.

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 230 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 of significant importance 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 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 evidently 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 2021 and Investment Strategy Consultant of the year 2021, respectively. We were also named as 1 of the top 10 flexible employers at the Flexibility Works Employer Awards.

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.

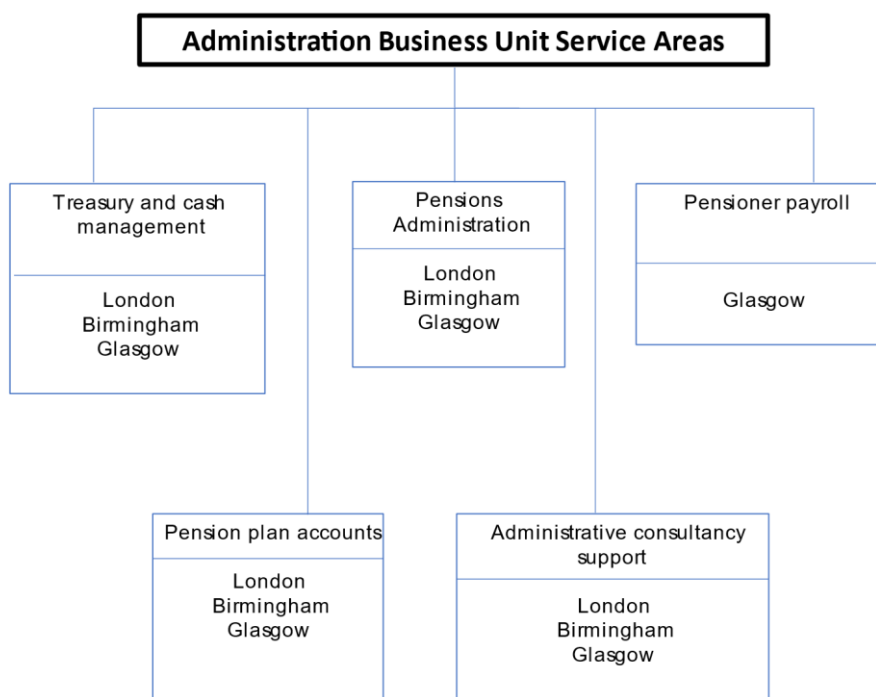
4 Pensions administration business unit

Administration service areas

Hymans Robertson have been providing third party administration services since 1984.

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 £10.0 million per annum turnover, employing over 200 staff, looking after 70 clients' pension schemes from our offices in London, Glasgow 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, treasury and cash management services and general administration to offer one-off consultancy support to Hymans Robertson's existing clients and other organisations where these activities are provided by in-house teams.

Operational systems

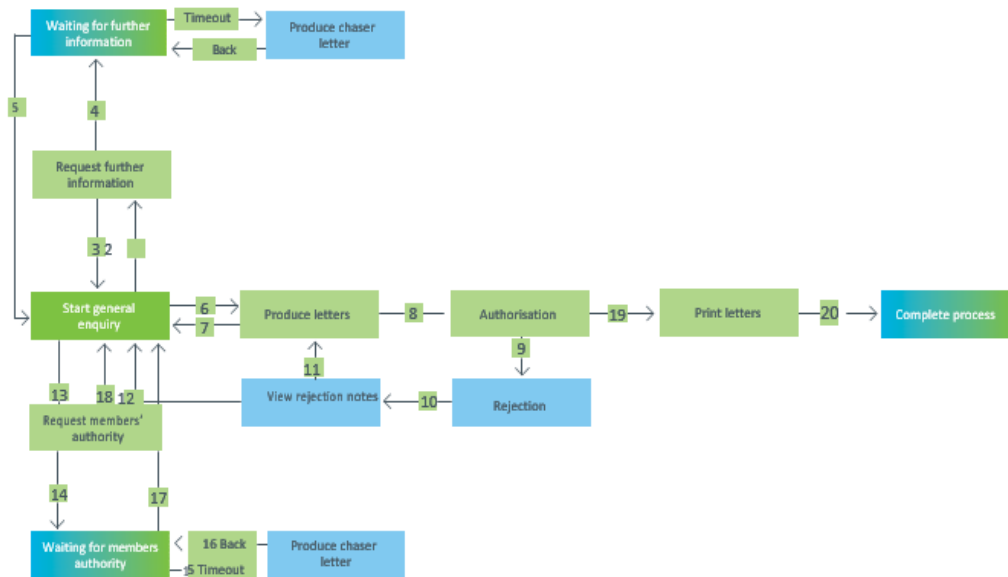
Our pensions administration and pensioner payroll services are delivered using the Civica Universal Pensions Management (UPM) software, our operating platform for all the administration and pensioner payroll functions. The UPM system represents the latest generation of pensions administration software 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.

A workflow process map is illustrated below:



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 pension plan accounting provider is Profund Aviary Professional.

Our treasury and cash management service is recorded through the use of a cashbook which is a Microsoft Excel document that we have created and which we maintain internally.

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 7 of this report.

5 Service auditor's assurance report on internal controls to the Partners of Hymans Robertson LLP



Crowe U.K. LLP
Chartered Accountants
Member of Crowe Global
55 Ludgate Hill
London EC4M 7JW, UK
Tel +44 (0)20 7842 7100
Fax +44 (0)20 7583 1720
www.crowe.co.uk

Service Auditor's assurance report on control activities to the Partners of Hymans Robertson LLP

Use of report

This report is made solely for the use of the members, as a body ("the Partners"), of Hymans Robertson LLP ("Hymans Robertson"), and solely for the purpose of reporting on the control activities of Hymans Robertson, in accordance with the terms of our engagement letter dated 25 January 2022 attached in the Appendix.

Our work has been undertaken so that we might report to the Partners those matters that we have agreed to state to them in this report and for no other purpose.

Our report must not be recited or referred to in whole or in part in any other document nor made available, copied or recited to any other party, in any circumstances, without our express prior written permission.

We permit the disclosure of this report, in full only, by the Partners at their discretion to clients of Hymans Robertson using Hymans Robertson pension administration services ("Clients"), and to the auditors of such Clients, to enable Clients and their auditors to verify that a report by a service auditor has been commissioned by the Partners of Hymans Robertson and issued in connection with the control activities of Hymans Robertson, and without assuming or accepting any responsibility or liability to Clients or their auditors on our part.

We also permit the disclosure of this report, in full only, by the Partners to those clients of Hymans Robertson not receiving pensions administration services or to prospective clients of Hymans Robertson, provided that the intended recipient must sign the 'hold harmless' letter referred to in our Engagement Letter and return it to us prior to receiving a copy of our report.

To the fullest extent permitted by law, we do not accept or assume responsibility to anyone other than the Partners as a body and Hymans Robertson for our work, for this report or the conclusions we have formed.

Subject matter

This report covers solely the control activities of the pensions administration function of Hymans Robertson as described in section 7 of your report during the year ended 31 January 2022. Control activities are processes designed to provide reasonable assurance regarding the level of control over Clients' assets and related transactions achieved by Hymans Robertson in the provision of pension administration activities by Hymans Robertson.

The Partners' responsibilities and statement are set out in section 2 of your report. Our responsibility is to form an independent conclusion, based on the work carried out in relation to the control activities of Hymans Robertson's pension administration function carried out at the Birmingham, Glasgow and London offices of Hymans Robertson and Club Vita (limited to restricting access to systems and data) as described in the Partners' report and report this to the Partners of Hymans Robertson.

Our independence and quality control

We have complied with the independence and other ethical requirements of the Institute of Chartered Accountants in England and Wales (ICAEW) Code of Ethics, which includes the requirements of the Code of Ethics for Professional Accountants issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

Crowe U.K. LLP is a limited liability partnership registered in England and Wales with registered number OC307043. The registered office is at 55 Ludgate Hill, London EC4M 7JW. A list of the LLP's members is available at the registered office. All insolvency practitioners in the firm are licensed in the UK by the Insolvency Practitioners Association. Crowe U.K. LLP is a member of Crowe Global, a Swiss Verein. Each member firm of Crowe Global is a separate and independent legal entity. Crowe U.K. LLP and its affiliates are not responsible or liable for any acts or omissions of Crowe Global or any other member of Crowe Global.

The firm applies International Standard on Quality Control 1 and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Criteria and scope

We conducted our engagement in accordance with International Standard on Assurance Engagements (ISAE) 3000 and ICAEW Technical Release AAF 01/20. The criteria against which the control activities were evaluated are the internal control objectives developed for service organisations as set out within the Technical Release AAF 01/20 and identified by the Partners as relevant control objectives relating to the level of control over Customers' assets and related transactions in the provision of pension administration activities. Our work was based upon obtaining an understanding of the control activities as described in section 7 of the report by the Partners, and evaluating the Partners' statement as described in section 2 to obtain reasonable assurance so as to form our conclusion.

Our tests are related to Hymans Robertson as a whole rather than performed to meeting the needs of a particular Customer.

Inherent limitations

Control activities were prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the control activities that may be relevant to each Client. Control activities designed to address specified control objectives are subject to inherent limitations and, accordingly, errors or irregularities may occur and not be detected. Such control activities cannot guarantee protection against (among other things) fraudulent collusion especially on the part of those holding positions of authority or trust. Furthermore, our conclusion is based on historical information and the projection of any information or conclusions in the attached report to any future periods would be inappropriate.

Conclusion

In our opinion, in all material respects:

1. section 7 of the accompanying report by the Partners describes fairly the controls procedures that relate to the control objectives referred to above which were in place during the year ended 31 January 2022;
2. the control activities described in section 7 were suitably designed such that there is reasonable, but not absolute, assurance that the specified control objectives would have been achieved if the described control activities were complied with satisfactorily; and
3. the control activities that were tested, as set out in section 7, were operating with sufficient effectiveness for us to obtain reasonable, but not absolute, assurance that the related control objectives were achieved during the year ended 31 January 2022.



Crowe U.K. LLP
Chartered Accountants
London

Date: 30 November 2022

6 Summary of control of objectives

1

Pensions administration

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

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.

5

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

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 in-scope systems is restricted to authorised individuals.

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

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

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

8

Maintaining integrity of the systems
Scheduling and internal processing of data is complete, accurate and within agreed timescales.

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

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.

Performance and capacity of in-scope systems are monitored and issues are resolved.

The physical IT equipment is maintained in a controlled environment.

11

Managing and monitoring compliance and outsourcing

Outsourced activities provided by Subservice Organisations are governed by contracts and service level agreements that are authorised and subject to regular review.

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


Club Vita - Information technology


1


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.

7 Control objectives and control activities

 Control applicable to DB only

 Control applicable to DC only

 Control applicable to both DB & DC

Note: 'DB' is an abbreviation for 'Defined Benefit'. 'DC' is an abbreviation for 'Defined Contribution'

1. Accepting clients

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

Following our appointment to provide pensions administration services, an initial letter of appointment will be provided by the client. We provide a template letter for this communication. Where Hymans Robertson is appointed to provide full services, the appointment documentation will be handled by the lead consultant and will include the administration services in the overall client agreement. This initial appointment is the trigger to commence the formal administration installation exercise. A key stage within the installation exercise is to establish and finalise the administration service schedules.

The Master Service Agreement (MSA) will be issued in draft, discussed with the client and its legal advisers as necessary, with a final version of the MSA being completed and signed on behalf of Hymans Robertson and the client prior to the commencement of the administration services.

If the MSA cannot be finalised before the proposed "live date" the services will be allowed to commence but based upon the terms of the initial appointment letter and our standard terms and conditions included within the proposals for services. We also have in place an interim Data Processing Agreement (DPA) until such time that the MSA is signed.

Key Controls

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



Crowe testing of control activities

Inspection

For a sample of new schemes we inspected the Master Service Agreement, and Data Processing Agreement where applicable, and ensured that this was signed on behalf of Hymans Robertson and the client. If the signed Agreement(s) have not been received prior to initiating the administration activity we obtained evidence that the client had confirmed the initial appointment.

No exceptions were identified

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.

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 or 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.

Key Controls

Tender review process, formal proposal for services, client verification and anti-money laundering form, new client set up form, new client installation checklist or detailed project plan and new client installation timeline are completed for each new client to ensure that all stages of the process are followed and documented.

Email sign-off is received and saved to UPM prior to data being released into the Live UPM environment.

Crowe testing of control activities

Inspection

➤ For a sample of new schemes we inspected the following documents and verified that these were completed as evidence of the stated processes being followed;

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

1 exception was identified, see page 4

The live data load is received and input to the data conversion software prior to processing on the UPM test platform. Testing is undertaken in a similar manner to the client test data load, and in addition, reconciliation reports are run. The mapping of membership data is 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.

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.

Key Controls

Control total testing is carried out 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.

For Defined Contribution Schemes, Unit Reconciliations are carried out.

Crowe testing of control activities

Inspection

For a sample of new schemes, we ensured control testing was 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 and unit reconciliations were performed for Defined Contribution Schemes.

No exceptions were identified

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

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 or alternatively 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 or the project manager 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.

Key Controls

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.

Crowe testing of control activities

Inspection

➤ For a sample of new schemes we obtained the installation checklist or the detailed project plan and inspected this for evidence of the installation timeline and verified that there was a sign-off of each section of the installation checklist or that the project plan was updated with a completion date.

No exceptions were identified

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

Team leaders and senior administrators are aware of the due dates for contribution receipts such that they will contact a client in advance if they consider there is any possibility of the late arrival of contributions if agreed with the client in advance.

The administration team receives notification from the client of contribution funding into the trustee bank account on a monthly basis. 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.

Following investment, a contract note is received from each investment manager.

There is a validation suite of reports within the defined contribution UPM process which tests the automated monthly allocation of investment units to members by comparison with contributions received for each individual member, the unit price supplied on a contract note and a control total of investment units. Where the unit price hasn't already been updated on UPM, a previous unit price is identified on the input screen to assess the validity of the latest transacted unit price. If the new unit price is out with expected tolerance this is flagged to the administrator to confirm whether the new unit price is correct.

A range of data validation tests are applied for each contribution processing cycle which highlight any areas for query or investigation. The reports are the same for a transfer-in process and the same validations are performed. 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 Bank Account analysis. This analysis is performed outside UPM and any residual 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 authorised by the Trustee.

Key Controls

Contributions are invested in accordance with client's instructions. The initial review is prepared and authorised and if there is a surplus, the investment is authorised by the Trustee.



Crowe testing of control activities

Inspection

For a sample of lifestyle investment switches we inspected evidence to ensure that the process was undertaken through the embedded workflow controls within the UPM system.

No exceptions were identified

The Internal Controls Monthly Report 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 Operations Leader 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 Operations Leader.

Key Controls

Internal Controls Monthly Reports are completed by each team leader and reports and 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.



Crowe testing of control activities

Inspection

For a sample of months we obtained the Internal Controls Monthly Reports for a sample of teams and ensured these were submitted at the end of each calendar month. We inspected the reports to ensure they included due dates for receipt and processing of contributions, monthly contribution investments and life style processing and that these reports were signed off by team leaders, administration managers for review and, where necessary, there is follow-up or sign-off by the Operations Leader.

No Exceptions were identified

Transfer-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 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.

Key Controls

Transfer-in benefits are processed in UPM by an administrator and authorised by a separate member of the team. The investment is actioned within 3 working days of receipt of reconciled funds.



Crowe testing of control activities

Inspection

For a sample of transfer-in's we inspected evidence that the investment had taken place within 3 working days of receipt of reconciled funds and that the investments were made in-line with member instruction. We also inspected evidence to ensure that the process was undertaken through the embedded workflow controls within the UPM system and the appropriate authorisation had taken place

No Exceptions were identified

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

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 Lifestyling or investment rebalancing. Member instructions are processed on receipt of a valid completed switch form or online request. Scheme/Plan Lifestyling is completed in line with client service orders.

Following receipt of an investment switch instruction a UPM Switch Matrix or PensionsWEB 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.

Key Controls

Investment switches are processed in UPM by an administrator and authorised by a separate member of the team. A switch is actioned within 5 working days of receipt of the request.

Crowe testing of control activities

Inspection

➤ For a sample of investment switches we inspected evidence that the switch was requested by a Scheme member, actioned by a member of the administration team, authorised by a separate team member and complete within 5 working days.

No exceptions were identified

Lifestyle investment 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 Lifestyling 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 dependant on receipt of contributions, therefore, if contributions are being invested, at the time the Lifestyling process is generated, the investment of contributions takes priority and Lifestyling begins once the contribution process has been completed.

Key Controls

Lifestyle investment 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.

Crowe testing of control activities

Inspection

➤ For a sample of lifestyle investment switches we inspected evidence to ensure that the process was undertaken through the embedded workflow controls within the UPM system and that the UPM process was signed-off and completed.

No exceptions were identified

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

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.

Key Controls

Each UPM process is authorised by another person on-line at the member record level.

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. 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.

Crowe testing of control activities

➤ Inspection

For a sample of benefit payments and transfer values we inspected evidence as follows:

- ensured that the UPM processes required that another person authorised the transaction
- on-line at member record level;
- for manual calculations we ensured that there was evidence that these were independently checked and where appropriate peer reviewed. We also checked for evidence of checking on the calculation document;
- ensured there was evidence that all calculations were checked before payment processing
- ensured that benefits were paid within the agreed timescales ; and
- ensured the payments of benefits were
- accompanied with appropriate letters.

No exceptions were identified

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 warm up letter process this letter will be sent to the member in advance of their normal retirement date.

Key Controls

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.

Crowe testing of control activities

➤ Inspection

For a sample of members reaching retirement we inspected evidence that retirement quotes and options available had been sent on a timely basis.

No exceptions were identified

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.

Key Controls

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. The documents are checked and authorised by another member of the administration team with a full audit trail recorded within the UPM process.

Crowe testing of control activities

➤ **Inspection**
For a sample of death benefits paid which were insured, we inspected evidence that death claims were made to the insurer.

No exceptions were identified

UPM retirement & death processes have embedded controls to ensure that new pensioners and beneficiary pensioners may only be created as a result of processing retirements or deaths for existing active, deferred or pensioner members. In addition, in order to create a new pensioner or beneficiary pensioner payroll record, authorisation has to 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.

Key Controls

To create a new pensioner or beneficiary pensioner payroll record, authorisation has to 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.

Crowe testing of control activities

➤ **Inspection**
For a sample of new pensioners we inspected evidence that the creation of the new pension was authorised by a member of the administration team and a member of the payroll team.

No exceptions were identified

3 Maintaining financial and other records

3.1 Member records consist of up to date and accurate information

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 also annually through renewal and annual increase exercises. Such updates are processed by a member of the administration team and peer reviewed.

Key Controls

Updates to member records are processed by a member of the administration team and peer reviewed.

Crowe testing of control activities

Inspection



For a sample of member requests in respect of data changes we ensured that member records were processed by a member of the administration team and peer reviewed.

No exception was identified

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. Since March 2020 all post has been diverted to 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 Internal Controls Monthly Report.

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.

Key Controls

Annual renewal exercises are prepared and authorised within UPM.



Crowe testing of control activities

Inspection

For a sample of schemes we ensured that the annual renewal exercise for active members and pension increases for pensioner members were undertaken through specific workflow processes within the UPM system.

No exceptions were identified

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 stewardship reporting.

Key Controls

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 stewardship reporting.



Crowe testing of control activities

Inspection

For a sample of schemes we ensured membership statistics were extracted from the UPM system, reported to clients as part of the quarterly stewardship reporting and there was evidence of review of the quarterly reports by a senior member of the administration team.

No exceptions were identified

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 member of the administration team.

Key Controls

The reconciliation of membership is peer reviewed by a member of the administration team.



Crowe testing of control activities

Inspection

For a sample of schemes we inspected the annual reconciliation of membership records and we checked these for evidence of review.

No exceptions were identified

3.2 Requests to change member records are validated for authenticity

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, either through the pensionsWeb Employer Portal or via email, it is updated to match the information provided.

If the request is received from the Scheme member there are a number of steps the administrator must take, in following our document process, in order to verify the member and the legitimacy of the data change request before it is updated on the member record.

Upon receipt of a request via telephone the member is advised that we are unable to take the change of details over the telephone and the team member advises that the request must be in writing or by email and provides details of the additional ID we must receive.

The additional ID documents required is 1 item from each of the 3 lists detailed below (extract taken directly from the form issued to Scheme members).

List 1 – Proof of name	List 2 – Proof of address	List 3 – Proof of bank account
Current UK or EEA passport.	Current full UK or EEA photocard driving licence. (if not used as proof of name).	A statement from your bank or building society (dated within the last 3 months). For this purpose a copy of an online statement is acceptable.
Current full UK or EEA photocard driving licence.	Current full UK driving licence (old paper style – please note paper counterpart to photocard licence cannot be accepted) (if not used as proof of name).	
Current full UK driving licence (old paper style – please note paper counterpart to photocard licence cannot be accepted).	Letter from Department for Work & Pensions confirming entitlement to state benefits issued within the last 3 months (if not used as proof of name).	
Letter from Department for Work & Pensions confirming entitlement to state benefits (issued within the last 3 months).	Recent utility bill (issued within the last 3 months).	
HMRC document such as PAYE coding notice or statement of account (issued within the last 3 months).	Statement from a bank, building society, mortgage company or insurance company (issued within the last 3 months).	
EU or EEA member state identity card.	Local authority council tax bill for the current year.	

Once the additional ID&V documents are received, as long as they fit the requirements of our process, we are able to 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 with the UPM record.

We have also implemented an updated process to checks made for overseas ID&V using ID-Pal, which is an app for members to download and use. The additional overseas ID checks were introduced in September 2021.

Key Controls

ID checks are performed appropriately and ID is loaded to the UPM record before updates are made to a UPM record and before benefits are paid.

Crowe testing of control activities

Inspection



For a sample of data changes we obtained evidence that copies of the ID were obtained. We obtained evidence that the lexis nexis checks were undertaken. We obtained evidence that the above was imbedded into UPM and that it was signed off by another team member.

No exceptions were identified.

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

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

Bank reconciliation are undertaken and checked on a monthly basis, with the reconciliation date entered onto the Internal Controls Monthly Report. This report is reviewed and signed-off by each office administration manager who sample checks where necessary.

Key Controls

The bank reconciliation is recorded on the Internal Controls Monthly reporting control which is reviewed and signed-off by each office administration manager.

Crowe testing of control activities

Inspection



For a sample of Internal Controls Monthly Reports we checked for evidence of the date of the bank reconciliation being performed monthly and checked that the reports were reviewed and were signed off by team leaders, administration managers for review and, where necessary, there is follow-up or sign-off by the Operations Leader.

No exceptions were identified

Entries on the cash book are used as a source of input to the preparation of the quarterly stewardship report, which include dates of contributions and payments, to the clients, and also for the Annual Report and Financial Statements which are subject to audit by the clients, which include auditors.

Quarterly stewardship reports are compiled using both data extracted directly from UPM, such as membership statistics and work statistics, and data sources outwith UPM, such as the cashbook. Once drafted, the stewardship report is reviewed by a senior member of the administration team prior to sharing with the client.

Key Controls

The quarterly stewardship reports are drafted by a member of the team then reviewed and authorised by a senior member of the team.

Crowe testing of control activities

Inspection

➤ For a sample of quarterly stewardship reports we ensured that dates of contributions and payments were included and there was evidence of review of the quarterly reports.

No exceptions were identified

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

For a Defined Benefit scheme, investment transactions arise out of the cash management process where funds in excess of 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 signatories.

Key Controls

Surplus funds are signed-off by a checker who inspects evidence that these were recorded in the cashbook. The investment was signed off by an authoriser and a bank instruction form was raised and signed by two signatories.

Crowe testing of control activities

Inspection

➤ For a sample of investments in Defined Benefit schemes we ensured that these represented surplus funds as evidenced by a sign-off by a checker and inspected evidence that these were recorded in the cashbook. We also ensured that the investment was signed off by an authoriser and a bank instruction form was raised and signed by two signatories.

No exceptions were identified

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.

Key Controls

For the disinvestment of investments, an order instruction is raised, authorised and issued to an investment manager..

Crowe testing of control activities

Inspection



For a sample of disinvestments in Defined Benefit schemes and Defined Contribution schemes we verified that order instructions for disinvestments were raised and authorised.

No exceptions were identified

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 reconciliation are carried out monthly or in line with the reporting cycles of relevant investment managers where monthly reporting is unavailable. These unit reconciliation are reported as having been completed in the Internal Controls Monthly Reports.

Key Controls

Defined Contribution unit reconciliation are reported as having been completed in the Internal Controls Monthly Reports which is signed off by team leaders, administration managers for review and, where necessary, there is follow-up or sign-off by the Operations Leader.

Crowe testing of control activities

Inspection



For a sample of Defined Contribution unit reconciliation we checked that these had been completed and signed off on the Internal Controls Monthly Reports.

No exceptions were identified

Where we provide the Trustees with Annual Accounting services, the accounting records for Defined Benefit investments are reconciled to investment manager transaction statements on an annual basis as part of the Report & Accounts preparation. This involves reconciling the investment cash transactions through the Trustee bank account to the independently received investment manager confirmations via a control account on our accounting package. This is reviewed by the lead pension plan accountant as part of the wider review of the annual Report & Accounts prior to submission to the auditor.

4. Safeguarding assets

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

Member and scheme data are both physically and logically protected from unauthorised access.

Each office has a controlled entry system and a manned reception desk to monitor visitor movements.

Key Controls

Each office has a controlled entry system and a manned reception desk to monitor visitor movements.

Crowe testing of control activities

Inspection



Through enquiry we ensured there was a controlled entry system and a manned reception desk to monitor visitor movements.

No exceptions were identified

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.

Key Controls

Access requires layered passwords, each layer being controlled and administered separately.

Crowe testing of control activities

Inspection



We verified through observation that access to the system was controlled through layered password in accordance with job responsibilities.

No exceptions were identified

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.

Key Controls

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.

Crowe testing of control activities

Inspection



We verified through enquiry that scheme data held as hard copy was held in dedicated and secure filing areas when not in use.

No exceptions were identified

Historical hard copy member data is archived and held in secure storage with our approved off-site suppliers relevant to each office location. Member data originating prior to the installation of the UPM system is back scanned and stored at the member record level as required.

Key Controls

Historical hard copy member data is archived and held in secure storage with our approved off-site suppliers relevant to each office location.



Crowe testing of control activities

Inspection

We verified through enquiry that historical hard copy member data was archived and held with approved off-site suppliers relevant to each office location.

No exceptions were identified

Key Controls

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



Crowe testing of control activities

Inspection

For a sample of member data originating prior to the installation of the UPM system we ensured through enquiry and observation that this was back scanned and stored at the member record level as required.

No exceptions were identified

4.2 Cash in Scheme bank account is safeguarded and payments are suitably authorised

Payment processing is undertaken daily at each site with appropriate segregation of duties being applied. Preparation of a payment instruction is functionally segregated from authorisation.

Key Controls

Preparation of a payment instruction is functionally segregated from authorisation.



Crowe testing of control activities

Inspection

For a sample of bank payments we checked for evidence of separate personnel preparing and authorising the payments.

No exceptions were identified

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.

Key Controls

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.



Crowe testing of control activities

Inspection

For a sample of client bank accounts we ensured that these were established in the name of the trustees with a restricted list of Hymans Robertson signatories.

No exceptions were identified

Key Controls

Upper signing limits will be operated based upon client instructions and requiring client representatives to authorise payments above those agreed limits.



Crowe testing of control activities

Inspection

For a sample of client bank accounts where clients had requested upper signing limits we evidenced that the upper limits were applied to the payment authorisation system.

No exceptions were identified

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.

Key Controls

An automated warning process applies when the established lower and upper limits are exceeded which triggers a review and any action that may need to be taken.



Crowe testing of control activities

Inspection

For a sample of client bank accounts relating to defined benefit we ensured limits were reviewed and monitored as part of the monthly bank account reconciliation process and where appropriate we observed evidence of the automated warning process which applied when these limits are exceeded.

No exceptions were identified

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;
- 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.

Key Controls

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;
 - Final authorisation of the payment is completed by a fourth person, again independent of the administration process.
-

Crowe testing of control activities

Inspection



For a sample of electronic payments we checked for evidence of:

- separate members of the team having prepared and authorised the transaction;
- use of an authentication device as a separate process;
- submission of documentation and payment processing details to the administration team; and
- Transmission confirmation retained as a separate record.

No exceptions were identified

The alternative to making an electronic payment is cheque processing. Cheques are held in safe custody at a central location on each site, and are only accessible by approved persons. Cheque signatories are identified on authorised bank mandates which are updated as required, and a copy held at each site.

Key Controls

Cheques are held in safe custody at a central location on each site, and are only accessible by approved persons.



Crowe testing of control activities

Inspection

For a sample of client bank accounts we enquired as to what cheques were held and where they were held on each site being only accessible by approved persons.

No exceptions were identified

A cheque is prepared by the administration team or cash management team. 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 administration team or cash management team who scans a copy of the payment documentation into the UPM system at member.

Key Controls

Cheque register logs are maintained, as part of the post opening duties, in each location at our Glasgow office which log payee, amount, scheme and date banked. Cheques are scanned onto the UPM record then passed to Team Leader the Cash Management team, for banking, on the day received to ensure prompt paying in.



Crowe testing of control activities

Inspection

For a sample of cheques received we checked that they were banked promptly.

No exceptions were identified

Cheque register logs are maintained, as part of the post opening duties, at our Glasgow office which log 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.

Key Controls

Cheque register logs are maintained, as part of the post opening duties, in each location at our Glasgow office which log payee, amount, scheme and date banked. Cheques are scanned onto the UPM record then passed to Team Leader the Cash Management team, for banking, on the day received to ensure prompt paying in.



Crowe testing of control activities

Inspection

For a sample of cheques received we checked that they were banked promptly.

No exceptions were identified

At the end of a calendar month each team is required to submit to the site administration manager their Internal Controls Monthly Report 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 reconciliation are performed monthly. The centralised cash management unit undertakes reconciliation of their cash management accounts. Where an administration team has retained their cash management function, they perform the reconciliation. A sign-off stamp of both the doer and the checker is recorded in addition to the date of reconciliation. Since March 2020 most transactions are now signed-off using electronic signatures.

Key Controls

Where an administration team has retained their cash management function, they perform the monthly bank reconciliation. A sign-off stamp of both the doer and the checker is recorded in addition to the date of reconciliation. This date is then recorded on the Monthly Internal Controls Report.



Crowe testing of control activities

Inspection

For a sample of monthly bank reconciliation we ensured that these were completed and we inspected evidence of a sign-off stamp of both doer and checker and the date of the reconciliation. We also checked that these were recorded within the Monthly Internal Control Reports.

No exceptions were identified

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 accounts team, located at a separate office, undertaking 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.

Key Controls

Detailed checklists assist with both preparation and authorisation processes and include completion of a payroll reconciliation sheet for each payroll/payroll group which identifies changes between payroll periods.

A manual check is performed to compare each payroll total to the previous month and differences of more than 10% are investigated.

Crowe testing of control activities

Inspection

➤ We observed the preparation of a monthly payroll and the use of the checklists for procedural guidance.

For a sample of payrolls we obtained the manual checks performed to ensure that differences of more than 10% are investigated.

No exceptions were identified

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.

Key Controls

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.

Crowe testing of control activities

Inspection

➤ For a sample of monthly pension payrolls we inspected the reconciliation sheets for evidence of a quality sign-off stamp and identification of the BACS file name and creation date.

No exceptions were identified

Client payrolls have been processed individually and, apart from two clients (up to April 2021 for client and July 2021 for the second client), have been processed 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. Our testing indicates that these two clearing accounts are no longer being used from July 2021.

Key Controls

Client payrolls have been processed individually and, apart from two clients (up to April 2021 for client and July 2021 for the second client), have been processed 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. Our testing indicates that these two clearing accounts are still no longer being used from July 2021.

Crowe testing of control activities

Inspection

➤ For a sample of monthly reconciliation of the payroll clearing account we inspected evidence of sign-off.

No exceptions were identified

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

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 Internal Controls Monthly Reports 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.

Administration teams record receipt of contribution payments within the cashbook ledgers noting amounts and dates of payment.

Key Controls

Late or non payment of contributions are included on the Internal Controls Monthly Reports and communicated to the Scheme actuary and client. Non-payment or late payment is reported promptly by the administration team to the scheme actuary and the client.

Crowe testing of control activities

Inspection

➤ We enquired into any late or non-payment of contributions and ensured these were included in the Internal Controls Monthly Reports and communicated to the scheme actuary and client. For a sample of Internal Controls Monthly Reports we inspected the reports for any late payments of contributions and where applicable checked for evidence that the late payment of contributions were reported by the administration team to the scheme actuary and client.

No exceptions were identified

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

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.

Key Controls

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.

Crowe testing of control activities

Inspection

➤ For a sample of clients we tested to ensure any amendments to the delivery of services was as agreed with the client and the service line agreement amended accordingly.

No exceptions were identified

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 are able to monitor and sort work in accordance with due dates for completion and levels of priority.

Key Controls

Administration staff and team leaders work directly from electronic work trays within the system and are able to monitor and sort work in accordance with due dates for completion and levels of priority

Crowe testing of control activities

Inspection

➤ We verified through observation that administration staff and team leaders worked directly from electronic work trays within the system and were able to monitor and sort work in accordance with due dates for completion and levels of priority.

No exceptions were identified

Administration team leaders review workloads for their team members daily.

Key Controls

Administration team leaders review workloads for their team members daily.

Crowe testing of control activities

Inspection

➤ We verified through observation that administration team leaders reviewed workloads for their team members daily.

No exceptions were identified

SLAs are made available to clients, at the proposal for services stage, and are detailed within the MSA. Subsequently, upon request, SLAs will be shared with clients or where changes are to be made.

Key Controls

Service Level Agreements (SLAs) are made available to clients, at the proposal for services stage, and are detailed within the Master Service Agreement (MSA). and s Subsequently, upon request, SLAs will be shared with clients or where changes are to be made.

Crowe testing of control activities

Inspection

For a sample of clients we ensured target service standards were made available to them upon request or where changes were made.

No exceptions were identified

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 stewardship reporting which is explained elsewhere in this document.

Key Controls

All work recorded within the UPM system is allocated a target completion date and various reporting tools are available to monitor completion and performance standards.

Crowe testing of control activities

Inspection

We verified through observation that work recorded within the UPM system was allocated a target completion date and we observed the available reporting tools used to monitor completion and performance standards.

No exceptions were identified

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

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.

Key Controls

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.



Crowe testing of control activities

Inspection

We verified through enquiry that employees were trained in the formal and documented Risk Event reporting process procedures and we observed that employees had access to the reporting guidelines.

No exceptions were identified

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, 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.

The Operations Lead is updated verbally on a weekly basis on the ongoing position of events by the Quality Assurance team and which events have been escalated to Legal or Risk.

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 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.

Key Controls

Risk Events are rated 1 through to 5 with 5 being Critical. The Quality Assurance team (and Legal or Risk as required) work with the client team and the Operations Lead (for Risk Events 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.

Crowe testing of control activities

Inspection

For a sample of Risk Event reports we obtained evidence to ensure that these were copied to the Operations Lead (for Risk Events rated 3 or higher) and where appropriate the Client Director as required, we also verified through enquiry that these had been resolved and communicated to the client.

No exceptions were identified

In accordance with both our regulatory obligations and professional standards the client team and the management of the business strive to ensure the fair treatment of the client, including where applicable individual members, in resolving any issues.

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

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 onto the required data spreadsheet for submitting to the online Event submission portal. Prior to submitting the spreadsheet is reviewed by a senior member of the team and, once submitted, the client authorises the submission.

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.

Key Controls

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.



Crowe testing of control activities

Inspection

We obtained, for a sample, evidence of who has prepared and reviewed the PAYE information.

We also obtained evidence of who authorised the payment.

No exceptions were identified

Key Controls

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.



Crowe testing of control activities

Inspection

For a sample we obtained evidence of who has prepared and reviewed the RTI submission.

No exceptions were identified

Upon request from HMRC, we may be required to complete a Pension Scheme Return, however, as this is on request it is not a periodic report.

If a regulatory breach should occur; we would inform the Trustees and provide them with the factual details of the case in order for them to report the breach to The Pensions Regulator, however this is a rare occurrence and not a periodic report.

6. Reporting to clients

6.1 Periodic reports to participants and scheme sponsors are accurate and complete and provided within the required timescales

Quarterly (or at a frequency agreed with the client) stewardship 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 issued to coincide with client trustee meetings.

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.

Key Controls

Quarterly (or at a frequency agreed with the client) stewardship reports are prepared and checked prior to issue.



Crowe testing of control activities

Inspection

For a sample of schemes we obtained a sample of quarterly stewardship reports and inspected evidence of these being checked.

No exceptions were identified

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 for the production of 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.

Key Controls

Annual benefit statements are produced through the automated workflow processes within the UPM system. Benefit calculations are completed through the automated calculation routines within the UPM system.



Crowe testing of control activities

Inspection

For a sample of annual benefit statements we ensured that these were produced through the automated workflow and calculation routines from within the UPM system.

No exceptions were identified

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 TPA Administration 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 lifestyling 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.

Key Controls

SMPI are calculated by the administration team using the DC Illustration System and then independently verified by a checking spreadsheet built by the Actuarial SMPI team. The checking spreadsheet is then signed-off by the Actuarial SMPI team.



Crowe testing of control activities

Inspection

For a sample of of clients, the checking spreadsheet was obtained and confirmed that it was signed off by the Actuarial SMPI team.

No exceptions were identified

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

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.

Key Controls

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.

Crowe testing of control activities

Inspection

For a sample of Annual Reports and Financial Statements we checked for evidence of:

- the accounts being checked by another member of the accounts team prior to audit by the scheme's external auditors;
- use of the template document for accounts production; and
- the completion of an accounts status spreadsheet signed by the preparer and the reviewer.

No exceptions were identified

7. Restricting access to systems and data

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

Each office has a controlled entry system and a manned reception desk to monitor visitor movements.

Key Controls

Each office has a controlled entry system and a manned reception desk to monitor visitor movements.

Crowe testing of control activities

Inspection

Through observation we ensured there was a controlled entry system and a manned reception desk to monitor visitor movements.

No exceptions were identified

At each site, computer equipment, such as spare hardware and laptops, is maintained in secure areas with restricted access to authorised personnel only. A visitor requiring access to any restricted area, for example an engineer, is supervised by IT operational staff.

IT equipment including servers, routers and emergency standby facilities is located within locked rooms.

Key Controls

Computer equipment, such as spare hardware and laptops, is maintained in secure areas with restricted access to authorised personnel only. IT equipment including servers, routers and emergency standby facilities is located within locked rooms.

Crowe testing of control activities

Inspection

We verified through observation that computer equipment was maintained in secure areas. We verified through observation that IT equipment is located in locked rooms.

No exceptions were identified

Gas suppressant in the event of a fire has been installed in accordance with Health and Safety requirements where the design and construction of office accommodation permits.

Key Controls

Gas suppressants have been installed in accordance with Health and Safety requirements where the design and construction of office accommodation permits.

Crowe testing of control activities

Inspection



We verified through observation that gas suppressant in the event of a fire had been installed where the design and construction of the office accommodation permitted.

No exceptions were identified

Equipment is accessible only to those members of staff who require operational access and who are suitably authorised.

Key Controls

Equipment is accessible only to those members of staff who require operational access and who are suitably authorised.

Crowe testing of control activities

Inspection



We verified through enquiry that equipment was accessible only to those members of staff who required operational access and who were suitably authorised.

No exceptions were identified

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. Additionally, guidance was issued to all staff during the Covid-19 pandemic, regarding working from home and the use/maintenance of I.T equipment when specifically working from home.

Key Controls

Staff sign up to our internal Information Security Policies as part of their employment contracts.



Crowe testing of control activities

Inspection

We verified through enquiry that all staff had signed up to the internal IT policy and operational terms.

No exceptions were identified

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

Logical access will be granted to network and applications in accordance with the authorisation by IT operations and the relevant system support teams.

New user access is established by the IT support team following submission of a new starter form which must be authorised by the user's line manager and Human Resources.

Key Controls

New user access is established by a new starter forms which must be authorised by the user's line manager and Human Resources.



Crowe testing of control activities

Inspection

For a sample of new starter forms we inspected these for authorisation by the user's line manager and Human Resources, and ensured new user access was established by the IT support team.

No exceptions were identified

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.

Key Controls

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.



Crowe testing of control activities

Inspection

For a sample of leaver forms we inspected these for authorisation by the appropriate manager and ensured the leavers accounts were closed by the IT team.

1 exception was identified, see page 4

A monthly reconciliation of leavers is completed between the Human Resource records and the central IT records, ensuring that any discrepancies are investigated.

Key Controls

A monthly reconciliation of leavers is completed between the Human Resource records and the central IT records, ensuring that any discrepancies are investigated.



Crowe testing of control activities

Inspection

We inspected the latest monthly reconciliation of leavers between the Human Resource and central IT records to ensure that any discrepancies are investigated.

No exceptions were identified

Logical access by privileged users is restricted to those individuals with specific technical network and application job responsibilities and in line with their requirement to resolve issues arising.

A monthly report is run showing user access rights, this is sent to Head of IT and to line managers to check users have the correct level of access to system relevant to their job role. Privileged users have administrative rights on our systems and networks.

Key Controls

A monthly report is run showing user access rights, this is sent to Head of IT and to line managers to check users have the correct level of access to system relevant to their job role. Privileged users have administrative rights on our systems and networks.



Crowe testing of control activities

Inspection

We obtained a list of privileged users and ensured that these were in line with responsibilities.

No exceptions were identified

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

Key Controls

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



Crowe testing of control activities

Inspection

We verified through enquiry and observation that enforced changes to passwords occurred at periodic intervals in accordance with network and application settings.

No exceptions were identified

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

Clients do not have access to our In-scope systems and data, however some clients have access to the Employer Portal in pensionsWeb; a shared secure platform for improving collaboration with employers by streamlining information transfer and validation. Employers have a secure log-in to enable them to upload data files for the administration team to download and then upload to UPM. Data files include: auto-enrolment details, bulk loader - joiners, leavers, data changes, bulk loader - DC contribution files. The bulk loaders are where data is received for multiple members of the Scheme on the same data sheet. An administrator is able to load the data sheet to UPM, using a bulk loader process. The bulk loader process is authorised by another member of the team and, once authorised, the relevant data is either posted to each individual member record (such as for salary updates), or the relevant UPM process is started for each individual (such as a leaver matrix).

Administrators can view information and requests from an employer to help them to carry out various tasks across the whole scheme.

In October 2021 our new secure digital access portal, PRISM, successfully went live with our first client offering their 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:

- Stewardship – 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 team work tray

We initially had 6 clients who signed-up to PRISM from launch date and we expect more clients to sign-up over the course of 2022. As of the end of January 2022, 12 clients in total have lunched on PRISM.

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 an not pensionsWeb,

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

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.

Key Controls

Access to the network and 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.

Crowe testing of control activities

Inspection

We verified through enquiry that access to the system was controlled by the different layers which are controlled through individual usernames, passwords and levels of access granted are in line with job responsibilities.



No exceptions were identified

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.

IT processing is available daily in accordance with business requirements. Back-up activity is undertaken to comply with a daily and weekly schedule and is detailed below.

Tested in 10.1

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

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.

Key Controls

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.

Crowe testing of control activities

Inspection

For a sample of data transmissions and data transmissions of financial data including pension payroll and electronic banking we checked for the use of secure encryption algorithms, smart card technology or password protection as appropriate.



No exceptions were identified

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.

Key Controls

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.

Crowe testing of control activities

Inspection

We verified through enquiry that only authorised senior personnel can access and handle financial data and we obtained a listing of personnel with access rights and verified through enquiry the segregation of duties.

No exceptions were identified

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.

Key Controls

The BACS Bureau facility is accessed through internet-based software by authorised individuals who have been set up as either Approvers or Submitters.

Crowe testing of control activities

Inspection

We verified through enquiry and the testing of a sample of BACS payments that the BACS payment process is accessed through internet-based software by authorised individuals who have been set up as either Approvers or Submitters.

No exceptions were identified

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

Key Controls

A restricted list of authorised users only can effect 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.

Crowe testing of control activities

Inspection

For a sample of BACS payments we tested that the payment had been authorised in line with the restricted list of authorised users and we inspected the transmission confirmation document and the processing confirmation from BACSTEL-IP.

No exceptions were identified

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

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, and are monitored via Checkpoint's Smart Event

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 through Checkpoint's Smart Event. This includes the documentation of changes in the internal Service Desk, approval via Change Advisory Boards and testing where appropriate, with approval, testing and implementation notes retained in the Service Desk ticket.

Key Controls

Firewalls with IPS engines are installed at the network perimeter as security devices; these support a dedicated WAN and MPLS circuit setup between offices.

Firewall events (e.g. attempted hacking, logins at unusual hours) are monitored via Checkpoint's Smart Event.

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

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

Changes to, and monitoring of, firewalls are managed by the Checkpoint. Firewall changes are tested and approved before implementation, managed within service desk solution.

Crowe testing of control activities

Inspection

We verified through enquiry and observation of the LAN-WAN Architecture Map, and the firewall setup itself, that firewalls with IPS engines are implemented to protect the WAN/MPLS setup.

We verified through on-screen observation that there are Rule Base Policy documents and Firewall Management Policy documents in place, covering the security setup of the firewall and access points, and the governance of these.

We verified through observation of the firewall console that monitoring of the firewall performance is performed.

We verified through enquiry that changes to the firewall would follow the standard change management process including documentation on the internal Service Desk. We reviewed the Service Desk and noted no changes specifically to the firewall which could be tested. We verified through observation of a sample of other changes, that changes are tested and approved prior to implementation, and that documentation of these processes are retained (see control 9.3).

No exceptions were identified

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.

The threat from malicious electronic attack is mitigated by the installation of firewalls and anti-virus software. The anti-virus software we have installed scans any file prior to opening. Should any virus or mal-ware be detected, the software generates a report accessible by IT operations. Follow-up action is taken.

Key Controls

The threat from malicious electronic attack is mitigated by the installation of firewalls and anti-virus software.



Crowe testing of control activities

Inspection

We verified through enquiry and observation that firewall and anti-virus software was used and maintained.

No exceptions were identified

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. Adhoc penetration test area is also conducted on new applications before being released to live environments. The last year was conducted in October 2021.

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.

Key Controls

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 these reviews and tests are distributed internally to the appropriate management and client teams. 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. Refers to the above controls and results of the intrusion test.



Crowe testing of control activities

Inspection

We obtained the report from the October 2021 test and reviewed this for the conclusion referred to. We also obtained the action plan and reviewed this for recommendations for improvement and confirmed through enquiry that high priority concerns were addressed.

No exceptions were identified

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

Since 2019, we have had a hybrid storage solutions for emails, where the host for all email is Microsoft Azure (a cloud computing service operated by Microsoft for application management via Microsoft-managed data centres) not in our on premises servers. Prior to any email hitting a user's inbox, the emails are scanned by

Cisco Email Security and Microsoft Advanced Threat Detection for known vulnerabilities. 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 mal-ware detected will be automatically reported to Service Desk for resolution.

On all laptops and servers, Microsoft Defender is in use alongside CylanceProtect, 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.

Key Controls

All emails are first scanned by Cisco Email Security, before they are scanned again by Microsoft Advanced Threat Detection, before the email reaches the user's mailbox. 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. Any virus or mal-ware detected is automatically reported to Service Desk for resolution.

Removable devices are blocked by default, with autoplay disabled for any exceptions to this rule.

Crowe testing of control activities

Inspection

We confirmed via enquiry and onscreen observation that Cisco Email Security is in use as a Software as a Service (SaaS) product, and that this, in conjunction with the anti-virus software, will scan emails including hyperlinks, attachments to the email and IP addresses.

We verified through enquiry and observation that anti-virus software was used and maintained [covered in 8.4]

We verified through observation of the anti-virus software that threat definitions are updated daily, automatically, and that threats are automatically quarantined for review.

We verified through enquiry and onscreen observation that any threats are automatically reported to the support teams for review.

We verified through enquiry and observation through Group Policy that removable devices are locked/restricted with autoplay disabled and scanned upon connection.

No exceptions were identified

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.

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 new secure digital access portal, successfully went live with our first client in October 2021, offering their 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.

Before being released to the Live environment, PRISM underwent an extensive testing. The testing is performed by 2 permitted individuals on any work item that has been through development and comprises several steps, including; initial discussion with developer, tester, and BA/product owner to agree what needs to be tested and identify any possible impacts on the wider application; following completion of development, in the development environment, code is deployed to test.

Testing is carried out in a dedicated test environment, using non-live data to ensure that any development environment changes do not impact the test environment; testing against each work item is recorded on UPM, with test steps being passed or failed, screenshot and text evidence attached to the system; any failed step is investigated, the same process of development in development environment before handover to test environment, and formal test with evidence attached, is followed; once testing is complete code is approved to move to User Acceptance Testing (UAT), or Live, by 3 permitted individuals (1 from the TPA Systems Team and 2 from the Insights & Analytics Development Team). Neither of the 3 individuals are testers and testing cannot be promoted to the UAT environment by testers.

Testers do not have access to live data or applications, excepting demo client which has no connection to any live client.

Key Controls

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 3 individuals who are not involved in testing.

Crowe testing of control activities

Inspection

In relation to the development of PRISM, we obtained:

- evidence of the testing and approval of each test step (including where test steps had been failed and subsequently approved.
 - confirmation of the approval of the complete code being moved to UAT, or LIVE, environment by staff members as approved by the Operations Leader.
-

No exceptions were identified

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.

Key Controls

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.

Crowe testing of control activities

Inspection

For a sample of upgrades to the UPM system we obtained evidence of testing and approval prior to release to the live database.

No exceptions were identified

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.

Key Controls

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.



Crowe testing of control activities

Inspection

For a sample of client specific changes we obtained evidence of testing and sign off prior to release to the live database.

No exceptions were identified

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

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 sign 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.

Key Controls

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.



Crowe testing of control activities

Inspection

For a sample of new schemes we inspected the new client installation checklists to ensure procedures relating to data migration or modification had been undertaken.

No exceptions were identified

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

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 SCCM. Change control processes are in place for configuration changes, including software installations for servers.

Patch management is controlled using WSUS (Windows Service Update Service) on a monthly schedule and when required for critical updates. Server patching of critical and security updates is conducted monthly and managed by a combination of WSUS and SCCM. Workstation patching is also managed by WSUS, critical and security patches are deployed daily.

Key Controls

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).



Crowe testing of control activities

Inspection

We observed the Change Management Process documents in place to confirm they cover all types of changes, including authorisation, testing, approval and implementation processes for each type of change.

We obtained evidence that changes are documented in a Service Desk Platform including authorisation, testing and approval, in line with change type, prior to implementation.

We confirmed through enquiry and onscreen observation that administrative access to both WSUS and MECM levels are restricted to support staff.

We confirmed through enquiry and onscreen observation that both WSUS and MECM are in use in a collaborative setup for collection/download and deployment of changes to software, servers and endpoints.

We confirmed via enquiry and onscreen review that current update status of update groups is visible in the software, and that automated alerting is in place for failure in update rules or deployment.

No exceptions were identified

10. Recovering from processing interruptions

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

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.

Key Controls

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.



Crowe testing of control activities

Inspection

We obtained and reviewed the business continuity plan to ensure that it had been designed as described.

No exceptions were identified

When an incident has been identified, the Emergency Response Team is formed; the Emergency Response Coordinator 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 2021.

Key Controls

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.



Crowe testing of control activities

Inspection

We obtained the results of the tests carried out in the Edinburgh office as evidence that the Business Continuity Plan has been tested.

No exceptions were identified

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 2021.

Key Controls

IT recovery tests are undertaken annually. We use cloud based recovery solutions [see above] for our data and servers.



Crowe testing of control activities

Inspection

We obtained the results of the IT recovery test and reviewed for evidence of file restoration at each office.

No exceptions were identified

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

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 15 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.

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.

Key Controls

SAN to SAN replication is carried out between our Glasgow and London data centres daily.

Crowe testing of control activities

Inspection

For a sample of daily back-ups we:

- ensured that Hymans Robertson's two main datacentres were backed-up and replicated to the opposite geographically separate datacentre;
 - verified through enquiry that, where any errors have arisen from the daily back-up process, these were actioned by IT staff on the following morning.
-

No exceptions were identified

Key Controls

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.

Crowe testing of control activities

Inspection

For a sample of monthly back-ups we verified through enquiry that, where any errors had arisen from the monthly back-up process, these were actioned by IT staff on the following morning.

For a sample of monthly back-ups we verified through enquiry that monthly back ups, were securely stored in the cloud.

No exceptions were identified

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

All production hardware is implemented in a highly available configuration. Servers have full HA configuration for power and cooling. 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 alerts on security threats and vulnerabilities from various installed sources (Microsoft / Checkpoint / Cisco). We use a number of event management tools that monitor snmp traps and syslogs for operational incidents, such as failure or loss of service.

Key Controls

A Security Incident Reporting Policy is used to govern processes around network intrusion incidents; this is supported by automated alerts from installed systems and event management tools to IT for monitoring and resolution

Contracts are in place with key system providers to allow 4 hour support responses if necessary

Crowe testing of control activities

Inspection



We confirmed through enquiry and observation of the Security Incident Reporting Policy that there is a formalised process to identify, manage and resolve network intrusion incidents.

We confirmed through enquiry and observation of key monitoring systems that there automated alerts are received on security threats and vulnerabilities, and monitoring is performed over snmp traps, syslogs, and operational incidents (such as loss of service).

We confirmed through review of the events log that these items are retained for audit log purposes.

We confirmed through enquiry and inspection of sampled key supplier contracts that support is in place with SLAs.

No exceptions were identified

10.4 Performance and capacity of in-scope systems are monitored and issues are resolved.

We operate systems resilience measures such as mirror servers, duplicate data centres and Active/Active configuration. Capacity management is in place to ensure that the resources are not over committed.

- General IT hardware and software issues are monitored and routed to a helpdesk facility. The request is prioritised as either low, medium or high priority and resolved within a defined timescale by either IT operational staff or a member of the TPA systems support team.

In relation to issues raised via the TPA Systems Support team:

- Timescales for issue resolution are not defined by fixed SLAs. Rather, issues are triaged on receipt and assigned a prioritisation** (normal/important/urgent/critical)
- Issues are then assigned to available resource based on priority order, but effort can vary significantly depending on issue scope.
- Urgent/Critical priority are allocated for commencement of resolution the same day.
- Important/Normal are allocated same day, but commencement of resolution may not be same day.
- **The originating user does have the opportunity to discuss and/or challenge the prioritisation assigned at triage, at which point we would re-assess and amend if agreement reached.

Key Controls

Requests are prioritised as either low, medium or high priority and resolved within a defined timescale by either IT operational staff or a member of the TPA systems support team.



Crowe testing of control activities

Inspection

For a sample of IT hardware and software issues we ensured that the request was prioritised as either low, medium or high priority and resolved within the defined timescale.

No exceptions were identified

Where an issue relates to the UPM system a relevant member of the TPA team is notified. The IT Operational Team identify the nature of the issue and pass to the systems support team to take appropriate action. Where an issue is identified as requiring resolution internally by the systems support team, a change control form is raised which provides appropriate details. The change is developed and then released into the test environment, prior to approval to run on the live platform.

Where the issue is identified as requiring resolution externally by the development of a software update by, or clarification from, the software provider, the issue is confirmed to the external provider. Once the external clients helpdesk systems have been aligned with their Developer Problem Logging system, their plan is to incorporate the logged issues into their version release notes. These can then be logged by Hymans to match to their issues originally raised.

Key Controls

Issues identified as requiring resolution internally by the systems support team, a change control form is raised which provides appropriate details. The change is developed and then released into the test environment, prior to approval to run on the live platform.



Crowe testing of control activities

Inspection

For a sample of UPM requests we ensured a change control form was raised and the change was tested and approved before running on the live platform.

No exceptions were identified

10.5 The physical IT equipment is maintained in a controlled environment

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 the our in house and/or Azure data centres. Services exclusively hosted on our in house data centre in the UK will be 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.

Key Controls

IT equipment including servers, routers and emergency standby facilities is located within locked rooms.



Crowe testing of control activities

Inspection

We verified through enquiry that IT equipment including servers, routers and emergency standby facilities were located within locked rooms.

No exceptions were identified

11. Managing and monitoring compliance and outsourcing

11.1 Outsourced activities provided by Subservice Organisations are governed by contracts and service level agreements that are authorised and subject to regular review

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

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

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

Club Vita - Information Security

1 Restricting access to systems and data

1.1 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 in accordance with the Club Vita System Access Control Policy

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.

Key Controls

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.



Crowe testing of control activities

Inspection

We obtained the Systems Access Control Policy and for a sample of new joiners we obtained the submitted Electronic Data Security Form and ensured that these had been authorised by the relevant authorisers as specified in the System Access Control Policy.

No exceptions were identified

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.

Key Controls

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.



Crowe testing of control activities

Inspection

For a sample of leavers we reviewed the leaver forms to ensure they had been authorised by the appropriate line manager and the individual's access had been removed.

No exceptions were identified


A quarterly report is produced and reviewed by the Club Vita operations team to ensure only authorised Hymans Robertson users are able to access all Club Vita specific systems, networks and data and at the appropriate level of access.

Key Controls

A quarterly report is produced and reviewed by the Club Vita operations team to ensure only authorised Hymans Robertson users are able to access all Club Vita specific systems, networks and data and at the appropriate level of access.

Crowe testing of control activities

Inspection

 We obtained a sample of quarterly reports and reviewed for evidence of review by the Club Vita operations team.

No exceptions were identified


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.

Key Controls

Logical access by privileged users is restricted to those individuals with specific technical network and application job responsibilities.

Crowe testing of control activities

Inspection

 For a sample of users included in the quarterly reports we reviewed access levels to Club Vita systems and ensured access had been set up at the appropriate levels according to their specific technical network and job responsibilities.

No exceptions were identified


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

Key Controls

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

Crowe testing of control activities

Inspection

 For a sample of users we observed that access to the systems requires passwords. Through enquiry we confirmed that passwords are required to be changed at periodic intervals.

No exceptions were identified

- a. 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.

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.

Key Controls

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.

Crowe testing of control activities

Inspection

For a sample of clients using Club Vita we obtained evidence of the submission of a Club Vita Member Site Login Request to the Club Vita operations team.

No exceptions were identified

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.

Key Controls

A quarterly report of individual client users, roles and access levels is independently reviewed by the Club Vita operations team each quarter.

Crowe testing of control activities

Inspection

We obtained a sample of quarterly reports and reviewed these to ensure they include client users, roles and access levels and that the reports were reviewed by the Club Vita operations team.

No exceptions were identified

Key Controls

A quarterly report of individual client users, roles and access levels is independently reviewed by the Club Vita operations team each quarter.

Crowe testing of control activities

Inspection

For a sample of users included in the report we reviewed access levels to Club Vita systems and ensured access had been set up at the appropriate levels.



No exceptions were identified

Appendix

Reporting Accountant's letter of engagement and hold harmless letter

25 January 2022

Our ref: AP/LOH01073/RR

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

Dear Sirs

This letter sets out the basis on which we shall be pleased to act for you and includes your and our respective responsibilities.

Under 'Other Matters' below, we set out our maximum legal liability. This letter is subject to the annexed Terms of Business and these include other important details, including provisions that further limit the amount of our liability in certain circumstances. Please read this letter and the Terms of Business carefully, and raise with me any questions that you might have.

1. Scope of our work

You have asked us to act as service auditor to deliver services to you in connection with the Pension Administration function of Hymans Robertson LLP carried out at London Birmingham and Glasgow for the year ending 31 January 2022 and Club Vita (limited to restricting access to systems and data).

2. Responsibilities of partners

2.1 The partners ("the Partners") of Hymans Robertson LLP ("the Organisation") in relation to which the reporting accountants' assurance 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 clients' assets and related transactions. The Partners' responsibilities are and shall include:

- a) acceptance of responsibility for internal controls;
- b) evaluation of the effectiveness of the service organisation's Control activities using suitable criteria; and
- c) supporting their evaluation with sufficient evidence, including documentation.

2.2 The Partners acknowledge and accept their responsibility for providing a written assertion about whether in all material respects, and based on suitable criteria:

- a) The Partners' description of the Organisation's system fairly presents the system that was designed and implemented throughout the specified period;

Crowe U.K. LLP is a limited liability partnership registered in England and Wales with registered number OC307043. The registered office is at 55 Ludgate Hill, London EC4M 7JW. A list of the LLP's members is available at the registered office. Authorised and regulated by the Financial Conduct Authority. All insolvency practitioners in the firm are licensed in the UK by the Insolvency Practitioners Association. Crowe U.K. LLP is a member of Crowe Global, a Swiss verein. Each member firm of Crowe Global is a separate and independent legal entity. Crowe U.K. LLP and its affiliates are not responsible or liable for any acts or omissions of Crowe Global or any other member of Crowe Global.

- b) The controls related to the control objectives stated in management's description were suitably designed throughout the specified period to achieve those control objectives; and
 - c) The controls related to the control objectives stated in management's description operated effectively throughout the specified period to achieve those control objectives.
- 2.3 This written assertion will be included in, or attached to, the Partners' description of the Organisation's system, and provided to user entities as part of the final report issued by management.
- 2.4 In drafting this report the Partners have regard to, as a minimum, the criteria specified within the Technical Release AAF 01/20 issued by the Institute of Chartered Accountants in England and Wales but they may add to these to the extent that this is considered appropriate in order to meet clients' expectations.

3. 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 Organisation's Pension Administration function carried out at the specified business units of the Organisation at London, Birmingham, Glasgow and Club Vita (limited to restricting access to systems and data) as described in the Partners' report and report this to the Partners.

4. Scope of the service auditors' work

- 4.1 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 which will be set out in an appendix to our report.
- 4.2 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 AAF 01/20 and ISAE 3402.
- 4.3 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.
- 4.4 We may seek written representations from the Partners in relation to matters on which independent corroboration is not available. We shall seek confirmation from the Partners that any significant matters of which we should be aware have been brought to our attention.
- 4.5 Our objective will be to conduct an examination that will include procedures to obtain reasonable assurance, in all material respects and based on suitable criteria, to enable us to express an opinion (Type II Reporting Accountant's Assurance Report) as to whether:
- a) The Partners description of its system fairly presents the system that was designed and implemented throughout the specified period and the aspects of the controls that may be relevant to a user organisation's internal control, as it relates to an audit of financial statements;
 - b) The controls included in the aforementioned description were suitably designed throughout the specified period to provide reasonable assurance that the control objectives specified in the description, would be achieved if the described controls were complied with satisfactorily; and
 - c) Such controls were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives were achieved during the specified period.
- 4.6 The control objectives for this examination are specified by the Partners. In conducting the examination we will examine on a test basis, evidence supporting the Partners' description of

4.7 controls, including the operating effectiveness of the related controls, and perform other procedures as we consider necessary in the circumstances to provide a reasonable basis for our report. Our examination will not include other systems, controls, operations or services not specified herein including internal control at user organisations and, accordingly, we will express no opinion on such items.

5. Inherent limitations

5.1 The Partners acknowledge that Control activities designed to address specified control objectives are subject to inherent limitations and, accordingly, errors or irregularities may occur and not be detected. Such procedures cannot guarantee protection against fraudulent collusion especially on the part of those holding positions of authority or trust. Furthermore, the opinion set out in our report will be based on historical information and the projection of any information or conclusions in our report to any future periods will be inappropriate.

6. Use of our report

6.1 Our report will, subject to the permitted disclosures set out in this letter, be made solely for the use of the Partners of the Organisation, and solely for the purpose of reporting on the internal controls of the Organisation, in accordance with these terms of our engagement.

6.2 Our work will be undertaken so that we might report to the Partners those matters that we have agreed to state to them in our report and for no other purpose.

6.3 Our 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 our express prior written permission. We permit the disclosure of our report, in full only, to clients of the Organisation using the Organisation's Pension Administration services ("Clients") and to the auditors of such Clients, to enable Clients and their auditors to verify that a report by a service auditor has been commissioned by the Partners of the Organisation and issued in connection with the internal controls of the Organisation without assuming or accepting any responsibility or liability to them on our part.

6.4 Should the Organisation wish to provide a copy of our report to those clients not receiving either Pension Administration services or to prospective clients of the Organisation ("Other Clients"), we will consent to our report being provided to Other Clients on the following basis:

- a) The report must be provided in whole; and
- b) The intended recipient must sign the attached 'hold harmless' letter and return it to us prior to receiving a copy of our report.
- c) The report may be included on the Organisation's website subject to the agreement of suitable wording setting out the terms which the user must accept prior to viewing the report.

6.5 To the fullest extent permitted by law, we do not and will not accept or assume responsibility to anyone other than the Partners as a body and the Organisation for our work, for our report or for the opinions we will have formed.

OTHER MATTERS

7. Limitation of liability

7.1 Our aggregate liability in respect of all claims by you under or in connection with this Contract shall be limited to the amount of £1,000,000. This limit shall apply to any and all causes of action against us in respect of or arising from or in any way connected with our engagement by you. However, we never seek to exclude or restrict our liability to the extent that we cannot do so by law for any reason, or any liability for our fraud or dishonesty. If you wish to discuss this or other provisions before we carry out work for you, please let us know.



8. Fees

- 8.1 Our fees are calculated on the basis of the time spent on your affairs by the partners and staff and on the levels of skill or responsibility involved.
- 8.2 Our fees will be billed in accordance with an agreed schedule.
- 8.3 If we need to do work outside the responsibilities outlined in our engagement letter, we will advise you in advance. This will involve additional fees. Accordingly it is in your interest to ensure that your records etc. are completed to the agreed stage.

9. Terms of Business

- 9.1 The Terms of Business accompanying this letter contain further information about the basis on which we will be pleased to carry out work for you. In the event of a conflict between the Terms of Business and what is set out in this letter, this letter will prevail.

10. Confirmation of your agreement

- 10.1 Please let me know if you have any questions in relation to this letter and the Terms of Business. If you are content with them, then would you please confirm your agreement by signing and returning one of the enclosed copies.
- 10.2 If I do not hear from you regarding this letter but it is clear that you wish us to proceed with the work, then this letter and the Terms of Business will govern the terms of our engagement.

Yours faithfully

Crowe U.K. LLP

AGREEMENT OF TERMS

I acknowledge receipt of this letter, which together with the Terms of Business fully records the agreement between us concerning your appointment to carry out the work described in it.

Name Gary Evans..... Signed

Position Head of TPA..... Date 25 March 2022.....

For and on behalf of the Partners of Hymans Roberson LLP

TERMS OF BUSINESS

1. Definitions

1.1 In these Terms of Business and any associated engagement letter:

1.1.1 "We" means Crowe U.K. LLP, and shall include any successor or assignee;

1.1.2 "You" means the person or company with whom the Contract is agreed and that is named as such in the engagement letter;

1.1.3 "Contract" means the terms of engagement agreed between Crowe U.K. LLP and you to which these terms of business relate and into which they are incorporated;

1.1.4 "Services" means the services we agree to provide you with under the Contract, as set out in the engagement letter.

2. Limitation of liability

2.1 We never seek to exclude or restrict our liability for our fraud or dishonesty, or otherwise to the extent that we cannot do so by law for any reason.

2.2 We accept that we owe you a duty of care to provide the Services with reasonable skill and care, regardless of whether the people we decide to use are members or employees (who may also be described as 'partners') of Crowe U.K. LLP or agents or sub-contractors retained by us. You in turn agree that you will not bring any claim based on any cause of action in respect of or in any way connected with the Contract against anyone other than Crowe U.K. LLP.

2.3 Where we are liable to you, and in addition any other person is also liable to you, or any such person or you have caused or contributed to the same loss or damage for which we are liable, either in whole or in part, then our liability shall be limited to such amount as is just and equitable having regard to the extent to which each of us and/or such other person is liable for and/or has otherwise caused or contributed to such loss or damage. For the purposes of this clause, the liability for and/or cause or contribution of any such other person shall be determined by disregarding any limitation, exclusion or restriction of legal liability or any inability to pay or insolvency, even if it means that you cannot recover any compensation from such other person.

3. Crowe Global and its member firms

3.1 Crowe U.K. LLP is a member of Crowe Global, a Swiss Verein. Each member firm of Crowe Global is a separate and independent legal entity. There is no ownership, agency, partnership or control relationship amongst any of Crowe Global and its member firms. Crowe Global does not perform

services and you agree that you will not bring a claim against it.

3.2 It is possible that we may retain another member firm of Crowe Global to act for us as a sub-contractor in providing the Services to you under this Contract. In that event, we accept that we owe you a duty of care to provide the Services for which we have retained that other member firm as a subcontractor, as set out in Clause 2.2, and you in turn agree that you will bring any claim against us and not against that other member firm, as set out in Clause 2.2.

3.3 If we have not retained another member firm as a sub-contractor, then you agree that any services that may be provided to you by another member firm are separate from the Services provided by us under this Contract. You will be responsible for entering into a separate contract of engagement with that other member firm, on such terms as you and that other member firm may agree. You agree that we shall not under any such circumstances be responsible or liable in any way whatsoever for any acts or omissions of Crowe Global or of any other member firms of Crowe Global.

4. Responsibility to third parties

4.1 We shall provide the Services for your exclusive use and for the purpose for which you engage us, and you agree that you will not disclose our advice or the product of our Services to anyone else without our specific written agreement.

4.2 We do not accept any responsibility to anyone other than you ("third party") for any aspect of our Services, whether because any work of ours is made available to the third party or for any other reason.

4.3 To the extent that the law imposes on us any responsibility to any third party even though we do not accept that, our liability to that third party shall be limited in accordance with the "Limitation of liability" section of the engagement letter. You therefore agree that you will share a single limit of liability as set out in those provisions in the event that we have a liability to you and to a third party.

5. Nature of our Services

5.1 You acknowledge that we will rely on information and documentation provided to us by you, your management, employees and third parties in the course of our work. We will not be responsible for the consequences of any deficiency in the information or documentation provided to us, whether as a result of it being false, misleading or incomplete. You agree to inform us if you are or become aware of anything inaccurate or misleading in respect of information or documentation provided to us.

5.2 Except as expressly agreed in the description of the Services in the engagement letter, our work will not be an audit as conducted in accordance with applicable auditing standards. Unless expressly agreed, we will not seek to verify the accuracy of

- 5.3 the information provided to us in the course of carrying out our Services, and we will not seek to or be responsible for detecting fraud by you or by your management, employees or third parties. We shall satisfy ourselves that the information provided is consistent with other information provided to us, but we will otherwise generally accept the explanation and assurances we receive from the partners, officers and employees of the entity that is the subject of the Services under this Contract or other third parties in the course of our work.
- 5.4 It may be necessary or desirable to instruct other professional advisers or third party suppliers in connection with the Services, upon whom we may place reliance and/or in conjunction with whom we may carry out our work. You shall be responsible for the appointment of such other professional advisers or suppliers and for their fees and expenses. We shall have no liability for the non-delivery, non-performance or any acts, errors or omissions of such other advisers or suppliers (other than our express agents), regardless of any role that we may perform in relation to communications with such advisers or suppliers.
- 6. Fees**
- 6.1 You agree to pay our fees within 30 days from the date of the invoice.
- 6.2 Payment of our fees from a bank based outside the UK must be made via transfer to our bankers and must quote our invoice details.
- 6.3 We will claim for relief for any fees falling within the scope of the VAT Regulations 1995 (SI 1995/2518).
- 7. Non-payment of fees**
- 7.1 If you fail to pay our fees within 30 days from the date of the invoice we reserve the right:
- 7.1.1 to charge monthly interest on the unpaid amount at 5% over the Barclays Bank plc Base Rate in accordance with the Late Payment Legislation;
- 7.1.2 to suspend the Services and any other work which we are carrying out for you;
- 7.1.3 to take whatever legal remedy exists in order to obtain payment; and
- 7.1.4 to claim the cost of debt recovery.
- 8. Communicating with you**
- 8.1 Please let us know if you have a preferred method of communication e.g. telephone or email or letter. Unless we hear from you, we will use whatever mode of communication appears appropriate in the circumstances.
- 8.2 All email messages sent to us will, if properly addressed, arrive on the terminal of the person to whom they are addressed. Please be aware of the following points:
- 8.2.1 the firm is connected to the internet, but the exchange of email messages may be subject to delays outside of our control;
- 8.2.2 the safe delivery of email via the internet should not be assumed;
- 8.2.3 the confidentiality of email cannot be guaranteed.
- 8.3 Please ask about our secure portal solutions. Unless you ask us, we shall not encrypt or promise to password-protect any email or attachment sent by us to you.
- 8.4 You and we shall not be responsible for each other's loss or damage arising from any corruption or alteration, or any unauthorised interception, redirection, copying or reading, of emails including any attachments.
- 8.5 You and we shall not be responsible for the effect on each other's hardware or software (or any loss or damage arising from any such effect) of any emails or attachment which may be transmitted by the other.
- 8.6 The recipient is responsible for carrying out a virus check on attachments.
- 9. Improving our service**
- 9.1 If at any time you would like to discuss with us how we could improve our service to you or you are dissatisfied with the service you are receiving, please let us know by contacting the engagement partner or Peter Varley, the Managing Partner of this office. Alternatively the Chief Executive of the firm Nigel Bostock, Crowe U.K. LLP, St Bride's House, 10 Salisbury Square, London, EC4Y 8EH.
- 9.2 Should our service be less than satisfactory we will take all reasonable steps to correct the situation. We undertake to investigate any complaints carefully and promptly and to report our findings to you.
- 9.3 If you are still dissatisfied you may take the matter up directly with the Institute of Chartered Accountants in England and Wales at:
- Professional Conduct Department
ICAEW
Level 1, Metropolitan House
321 Avebury Boulevard
Milton Keynes MK9 2FZ
- 10. Professional rules and practice guidelines**



- 10.1 We will observe the bye-laws, regulations and ethical guidelines of the Institute of Chartered Accountants in England and Wales and accept instructions to act for you on the basis that we will act in accordance with them. The requirements are available on the internet at www.icaew.com/membershandbook.
- 10.2 We are eligible to conduct audits under the Companies Act 2006 and details about our audit registration can be viewed at www.auditregister.org.uk, under reference number C001095468.
- 10.3 Details of our professional indemnity insurer can be found on our internet web site (www.crowe.com/uk/croweuk) on the legal information page, in accordance with the disclosure requirements of the Services Regulations 2009.
- 10.4 Our Services for you shall not be exclusive, and you agree that this Contract shall not prevent or restrict us from carrying on our business. We reserve the right during our engagement with you to act for other clients who may be competitors of yours or in respect of whom issues of commercial conflict may arise, subject to the Confidentiality section below.
- 10.5 Where a specific legal or ethical conflict of interest, actual or potential, is identified, and we believe that implementing appropriate procedures can properly safeguard your interests, we will promptly notify you and discuss the position with you. Please note that there may be circumstances where we are unable to fully explain all of the aspects of the conflict because of obligations that we owe to other clients or third parties. It may also not be possible to put effective safeguards in place, or you may not be content with the situation, in which case it may be necessary for us to terminate the Contract. You also agree to inform us immediately if you should become aware of, or believe that there may be, a conflict affecting our provision of the Services.
- 10.6 Our files are periodically reviewed by an independent regulator or quality controller as part of our on-going commitment to providing a quality service. The reviewers are bound by the same rules of confidentiality as our partners and staff.
- 11. Confidentiality**
- 11.1 We confirm that where you give us confidential information we shall at all times keep it confidential, except as required by law or as provided for in regulatory, ethical or other professional statements relevant to our engagement or for the purpose of notifying insurers concerning any actual or potential dispute relating to the Services.
- 11.2 You agree that we will be complying sufficiently with our duty of confidence if we take steps that we in good faith think fit to keep appropriate information confidential during and after our engagement.
- 11.3 You agree to reimburse any reasonable costs that we may incur in complying with any requirement for disclosure of your information that is imposed on us in any proceedings or regulatory process that does not involve any substantive claim or proceeding against us, provided that we promptly notify you in writing of any such requirement (to the extent we are legally permitted to do so) and that we reasonably cooperate with you in any efforts to protect against such disclosure.
- 11.4 You agree to keep confidential any methodologies and technology used by us to carry out the Services.
- 12. Data Protection**
- 12.1 When acting for you, we are a data controller in respect of any personal data you provide to us or to which we have access. This is because accountants and similar providers of professional services work under a range of professional obligations which oblige them to take responsibility for the personal data they process. For example if we detect malpractice whilst performing our services we may, depending on its nature, be required under our regulatory obligations to report the malpractice to the police or other authorities. In doing so we would not be acting on your instructions but in accordance with our own professional obligations and therefore as a data controller in our own right.
- 12.2 Where we and you are deemed in accordance with the data protection laws to be joint data controllers, you shall be liable for the personal data you process and we shall only be liable for the personal data we process.
- 12.3 You confirm that you have the right to supply personal data to us and this will not breach applicable data protection laws. Where you are providing personal data to us about a third party, for example a family member, a partner, a director (including a non-executive director), and/or any other type of member, business associate or third party, you confirm that you have their authority and express permission to provide us with their personal data.
- 12.4 Neither of us will by our act or omission put the other in breach of the applicable data protection laws.
- 12.5 Where we and you are joint data controllers, you should provide all relevant information to data subjects relating to the processing of their personal data (including the processing carried out by us) and to the exercise of their rights in relation to the processing of their personal data as required by the data protection laws ("Fair Processing Notice") and you will be the contact point for the data subject.
- 12.6 To enable us to discharge the services agreed under our engagement, and for other related purposes including updating and enhancing client records, analysis for management purposes and statutory returns, crime prevention and legal and regulatory compliance, we may obtain, use, process and disclose personal data about you or your entity, its officers and employees, as applicable. We confirm when processing data on your behalf we will comply with the relevant provisions of the applicable data protection laws.



- 12.7 Where we act as a data processor in relation to your personal data, we will:
- 12.8 process personal data:
- 12.8.1.1 for the purpose of performing our services and obligations to you; and
- 12.8.1.2 for such other purposes as may be instructed by or agreed with you or as otherwise notified in writing from time to time; and
- 12.8.1.3 in accordance with the applicable data protection laws;
- 12.8.2 implement appropriate technical and organisational measures to protect the personal data against unauthorised or unlawful processing and against accidental loss, destruction, damage, alteration or disclosure;
- 12.8.3 not otherwise modify, amend, remove or alter the contents of the personal data or subject to clause 12.1 above disclose or permit the disclosure of any of the personal data to any third party without your prior written authorisation;
- 12.8.4 adopt measures to maintain up to date records of our processing activities performed on your behalf which shall include the categories of processing activities performed, information on cross border data transfers and a general description of security measures implemented in respect of processed data;
- 12.8.5 unless otherwise required by data protection laws, or our own retention policy, we will return or delete all personal data upon the termination of our relationship with you;
- 12.8.6 adopt measures to ensure that only those personnel who need to have access to your personal data are granted access to it and that all of the personnel required to access your personal data are reliable and have been informed of its confidential nature;
- 12.8.7 not appoint a sub-processor without your prior written consent, not to be unreasonably withheld, and ensure an agreement is entered into with the relevant sub-contractor which includes terms which are substantially the same as the terms set out in this clause 12;
- 12.8.8 where we transfer your personal data to a country or territory outside the European Economic Area, to do so in accordance with data protection laws (including for the avoidance of doubt entering into standard form contracts);
- 12.8.9 notify you without undue delay if we receive: (i) a request from a data subject to access your personal data; or (ii) a complaint or request relating to the data protection laws;
- 12.8.10 assist you should you need to carry out a privacy impact assessment;
- 12.8.11 notify you in the event we become aware without undue delay of any breach of the data protection laws; and
- 12.8.12 permit without charge, on an annual basis, and / or where you become aware of a data breach or alleged breach of the data protection laws by us, reasonable access to the relevant records, files, tapes, computer systems, for the purposes of reviewing compliance with the data protection laws.
- 12.9 When acting for you in a personal capacity how we process your personal data is described in our privacy notice. This is available on our internet page. We will tell you if, in our opinion, your instructions may breach the applicable data protection laws.
- 13. Ownership and retention of documents**
- 13.1 All correspondence and papers in our possession or control and generated for our internal purposes (including our working papers) or addressed to us relating to the Services or the subject matter of the Services shall be our sole property.
- 13.2 We retain copyright and other intellectual property rights in everything produced by us before or during the Services.
- 13.3 We will keep correspondence and other papers and electronic data relating to the Contract, for such period as we may consider reasonable or that is required by law, and for at least eight years. After that time, we may destroy them without further reference to you.
- 14. Termination**
- 14.1 In relation to Services as Auditor under any statutory provisions, you or we may terminate the Contract only in accordance with the provisions of the relevant Act or regulation. In relation to any other Services, you or we may terminate the Contract at any time by giving not less than 30 days' notice in writing. We shall be entitled to payment for any work performed in relation to the Services by us prior to such termination.
- 15. Miscellaneous**
- 15.1 Neither of us may transfer nor assign this Contract, or any rights or obligations under it, without the prior written consent of the other party.
- 15.2 Neither of us will be liable to the other for any delay or failure to fulfil obligations caused by circumstances outside our reasonable control.
- 15.3 This Contract replaces and supersedes any previous proposal, discussion, correspondence, representation or agreement between us in relation to the Services, and forms the whole agreement between us in relation to such Services.



- 15.4 Any variation to the Contract shall only be effective if it is agreed in writing between you and a member in Crowe U.K. LLP, and only if agreed by reference expressly to the specific term to be amended.
- 15.5 Upon the termination of this Contract, we shall be under no further obligation to perform any part of the Services. However, the provisions of many clauses of these Terms of Business will, by their nature, continue to apply notwithstanding termination.
- 15.6 Unless we both agree otherwise, these Terms of Business (as amended from time to time) will apply to any future instructions that you may give us.
- 15.7 If at any time any provision of these Terms of Business or any engagement letter is or becomes illegal, invalid or unenforceable in any respect under the law of any jurisdiction, then that shall apply to the minimum extent required and shall not affect or impair the legality, validity or enforceability in that jurisdiction of any other provision of these Terms of Business or any engagement letter.
- 16. Applicable law and enforcement**
- 16.1 Our Contract with you is governed by, and interpreted in accordance with the laws of England and Wales.
- 16.2 A person who is not a party to the Contract has no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any of the terms of the Contract. This clause does not prejudice you in relation to any right or remedy that exists independently of the Act.
- 16.3 However, clause 16.2 does not apply to members, employees, agents, sub-contractors and others who have the benefit of the exclusion of liability in their favour under clauses 2.2 and 3. Accordingly, such persons may enforce that exclusion in their favour under the Contracts (Rights of Third Parties) Act 1999.
- 16.4 The Courts of England and Wales shall have exclusive jurisdiction in relation to any claim, dispute or difference concerning this Contract and any matter arising from them. Each party irrevocably waives any right it may have to object to any action being brought in those Courts, to claim that the action has been brought in an inconvenient forum, or to claim that those Courts do not have jurisdiction.

Hold Harmless Letter

[To be printed on client's or prospective client's letterhead]

ACKNOWLEDGEMENT DOCUMENT

TO BE COMPLETED AND RETURNED TO HYMANS ROBERTSON LLP BY CLIENTS (1) NOT RECEIVING EITHER PENSIONS ADMINISTRATION SERVICES OR CLUB VITA SERVICES OR (2) PROSPECTIVE CLIENTS

To Hymans Robertson LLP (the "Service Organisation") and Crowe U.K. LLP ("the Service Auditors")

The undersigned accepts and agrees:

(1) that the Service Auditor's Assurance Report on the internal controls of the pensions administration services of the Service Organisation and Club Vita (limited to restricting access to systems and data) for the year to 31 January 2022 ("the Report"), has been prepared on the basis, and subject to the terms and conditions, set out in the Engagement Letter dated 25 January 2022 between the Service Organisation and the Service Auditor, a copy of which has been provided to us;

(2) that the Report has been provided to us to verify that a report by the Service Auditor has been commissioned by the Partners of the Organisation and issued in connection with the internal controls of the Organisation without assuming or accepting any responsibility or liability to us;

(3) that the Report will not be recited or referred to or disclosed, in whole or in part, in any other document or to any other party.

Acceptance

Agreed and accepted by _____(name of signatory) on behalf of

_____(name of company) who represents that he/she is authorised to accept these terms on its behalf.

Signed:

Position:

Date:

This communication has been compiled by Hymans Robertson LLP based upon our understanding of the state of affairs at the time of publication. It is not a definitive analysis of the subjects covered, nor is it specific to the circumstances of any person, scheme or organisation. It is not advice, and should not be considered a substitute for advice specific to individual circumstances. Where the subject matter involves legal issues you may wish to take legal advice. Hymans Robertson LLP accepts no liability for errors or omissions or reliance upon any statement or opinion.

Hymans Robertson LLP (registered in England and Wales - One London Wall, London EC2Y 5EA - OC310282) is authorised and regulated by the Financial Conduct Authority and licensed by the Institute and Faculty of Actuaries

for a range of investment business activities. A member of Abelica Global.

© Hymans Robertson LLP.

Hymans Robertson uses FSC

approved paper. FTSE is a

registered trademark of

London Stock Exchange Plc