# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>4</td>
</tr>
<tr>
<td>Report by the Directors</td>
<td>6</td>
</tr>
<tr>
<td>Controls assurance framework</td>
<td>7</td>
</tr>
<tr>
<td>Organisation overview</td>
<td>8</td>
</tr>
<tr>
<td>Statement of internal controls</td>
<td>15</td>
</tr>
<tr>
<td>Summary of controls tested</td>
<td>18</td>
</tr>
<tr>
<td><strong>Pensions Administration</strong></td>
<td></td>
</tr>
<tr>
<td>1. Accepting clients</td>
<td>19</td>
</tr>
<tr>
<td>2. Authorising and processing transactions</td>
<td>22</td>
</tr>
<tr>
<td>3. Maintaining financial and other records</td>
<td>27</td>
</tr>
<tr>
<td>4. Safeguarding assets</td>
<td>33</td>
</tr>
<tr>
<td>5. Monitoring compliance</td>
<td>36</td>
</tr>
<tr>
<td>6. Reporting to clients</td>
<td>40</td>
</tr>
<tr>
<td><strong>Information Technology</strong></td>
<td></td>
</tr>
<tr>
<td>7. Restricting access to systems and data</td>
<td>43</td>
</tr>
<tr>
<td>8. Providing integrity and resilience to the information processing environment</td>
<td>48</td>
</tr>
<tr>
<td>9. Maintaining and developing systems hardware and software</td>
<td>52</td>
</tr>
<tr>
<td>10. Recovering from processing interruptions</td>
<td>54</td>
</tr>
<tr>
<td>11. Monitoring compliance</td>
<td>56</td>
</tr>
<tr>
<td><strong>Report by the Reporting Accountants</strong></td>
<td>58</td>
</tr>
<tr>
<td>Engagement letter</td>
<td>61</td>
</tr>
<tr>
<td>Disclaimer letter re prospective clients</td>
<td>71</td>
</tr>
</tbody>
</table>

If you are receiving this Report in your capacity as a prospective new client (i.e. post 31 December 2014) of RPMI then your attention is drawn to the Disclaimer letter at the back of this Report which outlines the basis on which you have received this Report and the Reporting Accountants' Assurance Report therein.
Introduction
RPMI has been delivering high-quality pensions administration for over 45 years, providing both pensions and investment services to the Railways Pension Trustee Company Limited (RPTCL). As well as delivering for our parent company, we also offer third party administration, communications and employer covenant services to schemes and employers.

We are based at three sites in Coventry, Darlington and London, and are continuing to grow. We currently look after the pension needs of over 200 clients and care for over 500,000 scheme members.

This Internal Control Assurance Report outlines the specific control procedures that we have designed to support our business objectives. It underpins the work RPMI has undertaken over many years, and together with the Reporting Accountants’ Assurance Report, independently demonstrates the strength of our control environment which supports our organisation as we move forward into the future.

This is our eleventh report and it has been prepared having regard to the International Standard on Assurance Engagements 3402 (ISAE 3402) and the Institute of Chartered Accountants in England & Wales (ICAEW) Technical Release, ‘Assurance reports on internal controls of service organisations made available to third parties’, (AAF 01/06).
Report by the Directors

This report relates to the pensions administration services provided by RPMI Limited (RPMI) at its offices in Coventry and Darlington.

As Directors, we are responsible for the identification of control objectives relating to clients’ assets, liabilities and related transactions in the provision of pensions administration services and the design, implementation and operation of the control procedures of RPMI, 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.

The accompanying description has been prepared for clients who have used the pensions administration services and their auditors who have sufficient understanding to consider the description, along with other information including information about controls operated by clients themselves, when assessing the risks of material misstatement of clients’ financial statements.

Our system of internal control is based upon an ongoing process which is designed to identify the risks to the achievement of policies, aims and objectives; to evaluate the nature and extent of those risks; and to manage them efficiently, effectively and economically. This process is consistent with the guidance and principles of the UK Corporate Governance code issued by the Financial Reporting Council in September 2012. An outline of our internal control and assurance framework can be found on pages 7-14 of this report.

The specific control procedures that we have designed to achieve the identified control objectives are outlined on pages 19-56. There have been no changes to our control objectives during the period. The report by the Reporting Accountants can be found on pages 58-60.

We have evaluated the fairness of the description, the design suitability and effectiveness of RPMI’s control objectives having regard to the International Standard on Assurance Engagements 3402 (ISAE 3402) and the Institute of Chartered Accountants in England & Wales (ICAEW) Technical Release, ‘Assurance reports on internal controls of service organisations made available to third parties’, (AAF 01/06), and the criteria for pensions administration set out therein.

We set out in this report a description of the relevant control procedures, together with the related control objectives which operated during the year ended 31 December 2014, and confirm that:

i. the report describes fairly the control procedures that relate to the control objectives referred to which were in place throughout the year ended 31 December 2014;

ii. the control procedures described are suitably designed such that there is reasonable assurance that the specified control objectives would be achieved if the described control procedures were complied with satisfactorily; and

iii. the control procedures described were operating with sufficient effectiveness to provide reasonable assurance that the related control objectives were achieved during the specified period.

Signed on behalf of the Board of Directors

10 March 2015

Chris Hitchen
Chief Executive
Controls assurance framework

Organisational structure
RPMI is wholly owned by the Railways Pension Trustee Company Limited, RPTCL (the Trustee Company) and operates from three sites in Coventry, Darlington and London.

The RPMI family

RPMI
RPMI looks after all administration and trustee services for the Railways Pension Scheme (RPS) and a large number of third party clients. It looks after the needs of over 500,000 pension scheme members across a variety of schemes and industries. It is responsible for the pensions administration services including the collection of contributions, payment of pension benefits and communications with members.

RPMI Railpen
Based predominantly at the London site, RPMI Railpen supports the 100-plus employers within the RPS in relation to investment management, and currently manages over £20bn of assets for the Scheme, which is the sixth largest pension fund in the UK in terms of assets under management. ‘Railpen Investments Limited’ is the regulated FCA authorised entity permitted to carry out certain regulated investment business under an Investment Manager Agreement with RPTCL, however, we refer to investments generally as RPMI Railpen for the purpose of this document.

RPMI EPAL
In 2011, Electricity Pensions Administration Limited (EPAL) became part of RPMI and looks after 69,000 members across 16 sections of the Electricity Supply Pension Scheme (ESPS).

Based at our Coventry site, EPAL has specialised in supporting the electricity sector for almost ten years.

Internal control
The system of internal control is based upon an ongoing process designed to identify the risks to the achievement of policies, aims and objectives; to evaluate the nature and extent of those risks; and to manage them efficiently, effectively and economically. This process is consistent with the guidance and principles of the UK Corporate Governance Code issued by the Financial Reporting Council. A key element of this structure includes formally agreed clear definitions of the responsibilities and authority delegated to individual managers across all major activities, supported by a number of important committees, each of which operates in accordance with agreed terms of reference.

Governance structure
The Trustee Board comprises 16 independent directors, a third of whom retire by rotation every two years with a six-year term of office.
Supporting Committees of the Trustee Company

The Trustee Company and its Board are supported by a series of key sub-committees whose roles and responsibilities are summarised below.

Integrated Funding Committee
- Manages and agrees integrated funding plans for the railways pension schemes and their sections, incorporating consideration of employer covenant, investment strategy and funding issues.
- Monitors performance of individual schemes and sections against the integrated funding plan and decides on actions to be taken between the actuarial valuations.
- Manages the actuarial valuation process for the railways pension schemes, including the transfer value basis, schedules of contributions and recovery plans with sponsoring employers.
- Agrees section specific valuation assumptions.
- Decides employer covenant assessment criteria, monitors covenant and corporate activity between valuations.
- Considers and approves minor / non-contentious scheme-wide rule amendments.
- Approves the Statement of Investment Principles for individual schemes and sections.

Case Committee
- Considers and decides on individual cases not delegated to RPMI or to a Pensions Committee.
- Considers and decides on cases under the Independent Dispute Resolution procedure, Pensions Ombudsman and associated matters.

Defined Contributions Committee
- Decides all changes to individual DC sections and arrangements regarding contributions, benefits and associated matters.
- Defines the characteristics of investment fund choices to be offered to members and reviews these regularly, including default options.
- Oversees and receives regular reports on DC investment performance.
- Ensures the Trustee’s DC arrangements are compliant with statutory, regulatory and constitutional requirements and regularly monitors against these requirements.

Executive Committee
- Has oversight of the operation of RPMI.
- Approves the appointment of the Directors of RPMI and decides on their terms and conditions.

Audit Committee
- Appointment of the external auditor, the scope and planned programme of work and evaluating their effectiveness and independence.
- Financial reporting arrangements including reviewing accounting principles, policies and practices.
- Reviews the scope, planned programme of work and ongoing effectiveness of the Business Assurance function.
- Reviews the control and risk management systems.
RPMI Board

The RPMI Board is responsible for the approval and ongoing monitoring of business strategy, financial performance, monitoring client delivery, remuneration policies and ensuring we continue to meet legal and regulatory requirements. The Board comprises four Executive Directors including the CEO, and four Non-Executive Directors, and operates with two core functions: (1) Administration and Trustee Services and (2) Investments. These functions are supported by the Corporate Services, including Group IT, People and Finance. Our Business Assurance team provides independent oversight over RPMI’s control framework.

The Executive Directors of the RPMI Board make up the Executive Leadership Team (ELT). Meeting frequently, the ELT are responsible for executive decision making and strategic oversight on a day-to-day basis.

Supporting the ELT, our Organisational Leadership Team (OLT) includes senior leaders from across the business and is accountable for shaping the strategy, evaluating progress and solving business challenges.

Risk management framework

The Corporate Risk Policy outlines the risk management framework and provides the basis for measuring, controlling, monitoring and reporting risk across the business.

The Risk Policy is reviewed regularly by management and annually by the Trustee Company and provides a framework for managing risk on a day-to-day basis. The Risk Policy covers all aspects of the Trustee Company’s and its subsidiaries’ operations and includes the use of third party service providers. RPMI’s risk management framework is consistent with the International Risk Management Standard ISO 31000.

Risk Management Committee

The Risk Management Committee (RMC) co-ordinates and monitors the risk management process on behalf of the Trustee and the operating companies. It is chaired by the Finance & Corporate Services Director. The Committee includes representatives of executive management and invites members of the Audit Committee and Non-Executive members of the Boards of the operating companies to attend. It meets regularly with Business Assurance and the external auditors in attendance, to consider key business risks and assess how they have been identified, evaluated and managed, and the effectiveness of the internal controls associated with these significant risks.

The RMC’s specific duties include the following:

- determining the risk policy and acceptable level of risk;
- identifying, recording and prioritising current and potential risks;
- deciding actions to avoid, reduce, transfer or accept risks;
- raising the level of management awareness of and accountability for risks;
- developing and promoting risk management as part of the culture;
- providing a mechanism for the discussion and resolution of risk management issues; and
- reviewing the action plans for the identified risks and ensuring that these are given the appropriate sponsorship and support.

Risk identification, assessment and management

Risks are identified and regularly reviewed by management and Directors in a formal process facilitated by the Business Assurance team. Risks are evaluated by considering the likelihood of occurrence and the significance of the consequent impact on the business if they occur.

Each inherent and residual risk is assessed against a specific matrix and alert system. Inherent risk is the assessed risk before internal controls are applied. Residual risk is the assessed risk after the application of controls. Controls can be defined as any action taken by management, the Board or any other parties to enhance risk management and increase the likelihood that established objectives will be achieved.

Risk Registers

All key risks are recorded in a specific risk register of the Trustee, RPMI or RPMI Railpen, which provides a means of regularly reviewing the assessment of each risk.

The Risk Registers identify the following for each risk:

- a risk owner who has overall responsibility for the risk;
- a risk manager responsible for managing the risk on a day-to-day basis;
- key controls operating to mitigate the risk;
- an impact / likelihood assessment of the residual risk;
- as assessment of the current assurance provided by the existing controls / measures operating; and
- a risk treatment action plan with resolution dates.
**Controls assurance map**

In support of the Risk Registers and as an aid to managing risk, a controls assurance map has been developed for each identified risk.

The assurance map identifies the key controls supporting a particular risk and the source and quality of assurance provided by each control. The process provides the means to identify and address any gaps in the risk management process and provides comfort that risks are being managed and reported on.

The approach is based upon the ‘three lines of defence’ model as outlined below.

**First line of defence:**

This refers to the day-to-day controls that have been designed into systems and processes and the line management and supervision that ensures compliance and identifies breakdowns or other unexpected events or errors. These processes are supported by documented policies and procedures or in some cases specific projects.

**Second line of defence:**

This describes the committees and functions that provide oversight of the effective operation of the internal control environment. This includes committees receiving reports and management information concerning key business activities; for example, the Executive Leadership Team and the Organisational Leadership Team. The second line is reinforced by the monitoring functions of risk management through the RMC and the Compliance team.

**Third line of defence:**

This describes the independent assurance provided by Business Assurance, External Audit and / or any other independent source of assurance; for example, internal controls reporting.

Sitting outside the risk management processes of the first two lines of defence, its main roles are to ensure that these are operating effectively. Tasked by, and reporting to the Board and Audit Committee, it provides an evaluation of the effectiveness of governance, risk management and internal control to the governing body and senior management.

The 3 Lines of Defence Model

<table>
<thead>
<tr>
<th>First Line of Defence</th>
<th>Second Line of Defence</th>
<th>Third Line of Defence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management controls</td>
<td>Compliance</td>
<td>Business Assurance</td>
</tr>
<tr>
<td>Day-to-day management of risk</td>
<td>IT Governance</td>
<td>External Audit</td>
</tr>
<tr>
<td></td>
<td>Risk Management</td>
<td>Internal Controls Reporting</td>
</tr>
<tr>
<td></td>
<td>Quality</td>
<td></td>
</tr>
</tbody>
</table>
## Business Assurance

Business Assurance services, overseen by the Head of Business Assurance, are provided in-house by a dedicated team of four qualified accountants. Through the delivery of internal audit and consulting services, and the facilitation of RPMI's risk management framework, they provide an independent assessment of the adequacy of internal controls across all areas of the business. They assist RPTCL and its operating companies in accomplishing its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes.

Business Assurance governs itself by adherence to the Institute of Internal Auditors’ ‘Code of Ethics’, and the Institute’s ‘International Standards for the Professional Practice of Internal Auditing’ (Standards) constitute the operating procedures for Business Assurance.

Business Assurance remains independent of operational management, reporting functionally to the Chief Executive Officer and the Audit Committee.

An annual audit plan is prepared, which is designed to deliver a series of audit engagements based on an appropriate risk assessment and priorities that are consistent with the objectives of RPTCL and its operating companies. The planning process involves:

- identification of the ‘audit universe’ – a comprehensive list of potential auditable areas by service, function and / or major systems;
- understanding the strategy and business objectives of RPTCL and the operating companies;
- risk and controls mapping to identify key risks and controls; and
- taking account of the results of previous audit work, discussions with key employees and consideration of current risks identified through the risk management framework.

The audit plan is formally approved by the Audit Committee.

Execution of the plan is assisted by an automated audit process designed to achieve improvements in productivity and enhancements to the effectiveness of service delivery and reporting.

The Business Assurance service also provides assurance through a number of additional support measures, including due diligence and other reviews of the internal controls of potential and existing service providers and providing support for the maintenance of the various quality accreditations that RPMI has attained; for example, those relating to Information Security and Business Continuity.

### Information security

The RPMI Group Information Technology service is responsible for delivering a corporate-wide technology infrastructure including web services, systems development and project management support. The governance and internal control arrangements supporting these services are managed by the IT Governance Manager, who is a Certified Information Systems Security Professional (CISSP) and is also responsible for co-ordinating business continuity arrangements. The Group IT service has been accredited to the International Information Security Standard ISO 27001 since 2009.

RPMI takes its responsibilities for ensuring the security and integrity of our information seriously and all our systems are continually under review to ensure they meet best practice.

The Computer Users Handbook outlines the policies, controls and expectations of our employees in the use of our systems and, in conjunction with our Data Protection Policy and embedded physical and logical access controls, provides a framework for maintaining the security and integrity of the information we are responsible for.

The Handbook outlines specific procedures and protocols for internet access; email; social media; systems use; data protection; and remote devices. RPMI regularly appoints external consultants to conduct independent IT security reviews to ensure that our measures remain up to date and effective.
**Business continuity**

RPMI’s business continuity arrangements are co-ordinated by the IT Governance Manager, who is a member of the Business Continuity Institute (MBCI). The procedures designed to ensure continuity of normal business in the event of an incident are outlined in a Business Continuity Plan (BCP). The plan embraces our locations in Coventry, Darlington and London and all areas of the business. We are ISO 22301 Business Continuity Management accredited.

The Business Continuity Steering Group comprising senior cross functional membership ensures that our plans are regularly updated and tested. A Business Continuity team, comprising senior management representatives, is responsible for co-ordinating, managing and determining the recovery process in the event of an incident requiring a business continuity response.

All of our key critical systems and data are replicated at our secure remote storage site and a schedule of testing is undertaken throughout the year to ensure the replication remains effective.

In the event of a major incident, business critical computer processing and services will be transferred to the designated recovery site. Office facilities are maintained and communication links with other companies and external offices have been established. A programme of training and awareness sessions is provided to our employees to ensure we all have the relevant knowledge and understanding of RPMI’s business continuity arrangements to be able to effectively carry out our roles in the event of a disruption to normal working practices.

**Safeguarding assets**

There are a number of measures that we adopt to protect RPMI’s and our employees’ reputations and to safeguard our assets. In particular, there are formally agreed definitions of the responsibilities and authority delegated to individual managers across all business areas. This management structure is supported by appropriate segregation of duties across the roles of authorisation, custody, recordkeeping and reconciliation.

The Business Assurance team facilitates RPMI’s Fraud Policy and Response plan, ensuring that management is well prepared to deal with any fraud incidents efficiently and effectively. Fraud awareness sessions are provided to all employees to ensure they are fully conversant with the procedures to follow in the event of a suspected fraud.

Being committed to high standards of openness, probity and accountability, we have prepared a Confidential Reporting of Concerns Policy which is designed to provide employees with clear, procedural guidance on reporting concerns about any aspect of the business.

**Compliance**

We recognise our responsibilities to ensure that the activities of RPMI and our employees are carried out properly and with the utmost propriety and that our managers conduct their activity properly and in accordance with statutory and regulatory requirements.

To ensure both our FCA regulatory activities and non-regulated activities are carried out competently, RPMI has a dedicated Compliance function. Integral to this function is maintaining an awareness of the external environment to ensure regulatory and legislative changes which impact us are adequately dealt with in our operations.

In support of this objective, we issue a number of corporate procedural and policy documents to our staff, including: Code of Conduct; Confidentiality of Information; Hospitality and Gifts Policy; Anti-Money Laundering Procedures; and a Compliance Manual.

The Compliance team has implemented a programme of regular compliance checks to ensure that our policies, processes and procedures are operating effectively, and they report the results of these to the Board.

**Staff training and development**

At RPMI, our people are our greatest asset. Our commitment to employ and retain people of the highest quality is supported by the work carried out by our People team and the investment we place in structured training and development plans.

We maintain rigorous employee vetting procedures and provide formal induction programmes for all new starters. These are supplemented by an ongoing performance management programme involving objective setting; informal one-to-ones; objective review; and annual appraisal.
RPMi is dedicated to providing employees with training and development that ensures the achievement of RPMi objectives and strategy. We encourage training that best fits their role or other relevant professional accreditations including PMI (Pensions Administration), ACA, ACCA and CIMA (accounting), CIM (Marketing), PRINCE 2 (Project management) and MCSE (IT).
Statement of internal controls
Statement of internal controls

This section contains the statement of internal controls for RPMI for the year ended 31 December 2014. The objectives, processes and internal controls are identified for each functional area for Pensions Administration and Information Technology. These have been determined in conjunction with the guidance in the ISAE 3402 and ICAEW technical release AAF 01/06.

All tests of operating effectiveness of internal controls were undertaken for the year ended 31 December 2014, with additional testing during January and February 2015 by the Business Assurance team and the Reporting Accountants.

Control objectives

Pensions Administration

1. Accepting clients
   - Accounts are set up and administered in accordance with client agreements and applicable regulations.
   - Complete and authorised client agreements are operative prior to initiating administration activity.
   - Pension schemes taken on are properly established in the system in accordance with the scheme rules and individual elections.

2. Authorising and processing transactions
   - Contributions to defined contribution plans, defined benefit schemes, or both, and transfers of members’ funds between investment options are processed accurately and in a timely manner.
   - Benefits payable and transfer values are calculated in accordance with scheme rules and relevant legislation and are paid on a timely basis.

3. Maintaining financial and other records
   - Member records consist of up-to-date and accurate information and are updated and reconciled regularly.

4. Safeguarding assets
   - Contributions and benefit payments are completely and accurately recorded in the proper period.
   - Investment transactions, balances and related income are completely and accurately recorded in the proper period.
   - Scheme documents (deeds, policies, contracts, booklets) are complete, up to date and securely held.

5. Monitoring compliance
   - Contributions are received in accordance with scheme rules and relevant legislation.
   - Services provided to pension schemes are in line with service level agreements.
   - Transaction errors are rectified promptly and clients treated fairly.

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 law and regulations.

Regulatory reports are made if necessary.

**Information Technology**

7. **Restricting access to systems and data**
   - Physical access to computer networks, equipment, storage media and program documentation is restricted to authorised individuals.
   - Logical access to computer systems, programs, master data, transaction data and parameters, including access by administrators to applications, databases, systems and networks, is restricted to authorised individuals via information security tools and techniques.
   - Segregation of incompatible duties is defined, implemented and enforced by logical security controls in accordance with job roles.

8. **Providing integrity and resilience to the information processing environment, commensurate with the value of the information held, information processing performed and external threats**
   - IT processing is authorised and scheduled appropriately and exceptions are identified and resolved in a timely manner.
   - Data transmissions between the service organisation and its counterparties are complete, accurate, timely and secure.
   - Appropriate measures are implemented to counter the threat from malicious electronic attack (for example firewalls and anti-virus software).
   - The physical IT equipment is maintained in a controlled environment.

9. **Maintaining and developing systems hardware and software**
   - Development and implementation of new systems, applications and software, and changes to existing systems, applications and software, are authorised, tested, approved and implemented.
   - Data migration or modification is authorised, tested and, once performed, reconciled back to the source data.

10. **Recovering from processing interruptions**
    - Data and systems are backed up regularly, retained offsite and regularly tested for recoverability.
    - IT hardware and software issues are monitored and resolved in a timely manner.
    - Business and information systems recovery plans are documented, approved, tested and maintained.

11. **Monitoring compliance**
    - Outsourced activities are properly managed and monitored.
Summary of controls tested

Pensions Administration

<table>
<thead>
<tr>
<th>Title</th>
<th>Controls</th>
<th>Pages</th>
<th>Summary of results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accepting clients</td>
<td>11</td>
<td>19-22</td>
<td>No exceptions</td>
</tr>
<tr>
<td>Authorising and processing transactions</td>
<td>15</td>
<td>22-26</td>
<td>No exceptions</td>
</tr>
<tr>
<td>Maintaining financial and other records</td>
<td>21</td>
<td>27-33</td>
<td>No exceptions</td>
</tr>
<tr>
<td>Safeguarding assets</td>
<td>11</td>
<td>33-36</td>
<td>No exceptions</td>
</tr>
<tr>
<td>Monitoring compliance (Pensions Administration)</td>
<td>12</td>
<td>36-39</td>
<td>No exceptions</td>
</tr>
<tr>
<td>Reporting to clients</td>
<td>11</td>
<td>40-42</td>
<td>No exceptions</td>
</tr>
</tbody>
</table>

Information Technology

<table>
<thead>
<tr>
<th>Title</th>
<th>Controls</th>
<th>Pages</th>
<th>Summary of results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restricting access to systems and data</td>
<td>19</td>
<td>43-47</td>
<td>No exceptions</td>
</tr>
<tr>
<td>Providing integrity and resilience to the information processing environment</td>
<td>17</td>
<td>48-51</td>
<td>1 exception - control 8.2</td>
</tr>
<tr>
<td>Maintaining and developing systems hardware and software</td>
<td>8</td>
<td>52-53</td>
<td>No exceptions</td>
</tr>
<tr>
<td>Recovery from processing interruptions</td>
<td>7</td>
<td>54-56</td>
<td>No exceptions</td>
</tr>
<tr>
<td>Monitoring compliance (Information Technology)</td>
<td>1</td>
<td>56</td>
<td>No exceptions</td>
</tr>
</tbody>
</table>

A management response is provided for the reported exception.

The types of tests performed are briefly described below:

**Enquiry**

Enquiries were made through discussion with appropriate personnel in order to corroborate existing controls in place and to provide further affirmation / additional information relating to the control environment.

**Inspection**

Inspections undertaken on evidence gathered from the control environment. The types of inspection include:

- reviewing source documentation and authorisation at transactional level;
- inspecting records kept for evidence of performance, system documentation and job descriptions; and
- inspecting reports and the authenticity of any data held to source.

**Observation**

Observed the control environment and the existence of specific controls / applications in operation.

**Re-performance**

Re-performed the control or process to confirm the accuracy of the transaction. This included re-performing and undertaking independent calculations and comparing reconciling items to source documentation.
Pensions Administration

1. Accepting clients

Accounts are set up and administered in accordance with client agreements and applicable regulations.

The client take-on process commences with the establishment of an implementation team. A standard project plan provides the basis for the transition, with client specific activities incorporated where necessary. The plan is shared with the client and key milestone dates agreed. A project manager is appointed to oversee progress on the plan and regular governance meetings are held to provide the client with updates.

At the onset, the client is asked to complete a comprehensive scheme questionnaire to confirm scheme arrangements and also specify in greater detail the scope of the service provision.

During the transition period, an issues log is maintained, with issues prioritised and discussed at each project meeting. Active engagement with the incumbent administrator is sought to assist in the transition.

A Client Services Manager is appointed to the client and will be an active participant throughout the transition, remaining the key point of contact for the client following take-on.

<table>
<thead>
<tr>
<th>Detailed controls</th>
<th>Relevant exceptions ‘if any’</th>
<th>DB</th>
<th>DC</th>
</tr>
</thead>
</table>
| 1.1 An implementation team, with cross functional representation, is established to undertake a standard installation project plan. Key milestones within the plan are agreed with the client and monitored through Client Service Manager project reporting. | **Inspection**
Confirmed for a sample of client take-ons that an implementation team had been established and that project milestones were agreed with the client and were reported throughout the project.*

**No exceptions to the company’s procedures were noted.** | | |
| 1.2 The client oversees implementation progress and risk reports are used to identify implementation issues which are discussed at the regular project meetings. | **Inspection**
Confirmed for a sample of clients that the implementation was overseen by the client and risk reports had been discussed at project meetings.*

**No exceptions to the company’s procedures were noted.** | | |
| 1.3 A standard scheme information questionnaire is completed and verified by the client during the transition process. | **Inspection**
Confirmed for a sample of clients that a scheme information questionnaire had been completed.*

**No exceptions to the company’s procedures were noted.** | | |
<table>
<thead>
<tr>
<th>Detailed controls</th>
<th>Relevant exceptions ‘if any’</th>
<th>DB</th>
<th>DC</th>
</tr>
</thead>
</table>
| **1.4** All client services are administered under an agreed and signed service level agreement. | Inspection  
Confirmed for a sample of clients that a service level agreement was in place.*  
No exceptions to the company’s procedures were noted. | ![circle] | ![circle] |
| **1.5** For each client, a primary Client Services Manager is assigned to monitor adherence to the client agreement. | Inspection  
Confirmed for a sample of clients that a primary Client Services Manager had been assigned.*  
No exceptions to the company’s procedures were noted. | ![circle] | ![circle] |

Complete and authorised client agreements are operative prior to initiating administration activity.

All client agreements include a formal service level agreement and scope of the administration activity. Wherever possible, the agreement is signed prior to live administration. The in-house Legal team provides the necessary support to finalise the agreement as soon as is practical.

Once the contract has been signed, future variations to the client agreement require written agreement from the client and RPMI.

<table>
<thead>
<tr>
<th>Detailed controls</th>
<th>Relevant exceptions ‘if any’</th>
<th>DB</th>
<th>DC</th>
</tr>
</thead>
</table>
| **1.6** A pension administration agreement, which sets out the scope of services, is authorised by the client representative and RPMI. Prior to initiating administrative activity, a service level agreement is established. | Inspection  
Confirmed for a sample of clients that an agreement setting out the scope of services and agreed service levels was in place.*  
No exceptions to the company’s procedures were noted. | ![circle] | ![circle] |

* Underlying test performed by the Reporting Accountants  
** Underlying test performed by RPMI Business Assurance team, subsequently reviewed by the Reporting Accountants.
Pension schemes taken on are properly established in the system in accordance with the scheme rules and individual elections.

A data validation tool is used to validate data and identify anomalies in advance of migration to the administration system to ensure the data transfer is accurate and complete. At the request of the client, data cleansing is also carried out.

For DB schemes, a review of the scheme rules / deeds is undertaken to produce calculation specifications; where agreed with the client, the specifications are provided to the Scheme Actuary for approval. Sample test cases for each calculation type are performed and reconciled to the specification / system output.

Where the scheme includes a pensioner payroll, a series of parallel payroll running is executed prior to the live production run. Discrepancies which fall outside of an agreed tolerance are escalated to the client / ceding administrator for resolution.

The membership options and current unit holdings held by members in defined contribution (DC) plans are uploaded onto the administration system; this forms the basis for full unit reconciliations with the investment manager holding statements. Discrepancies are investigated with the manager / ceding administrator to enable an agreed unit holding at the point of live administration.

The lifestyle profile procedures document is produced in accordance with the DC plan’s default lifestyle strategy. The client is asked to approve the document and this forms the basis of the lifestyle matrix which is input within the administration system and enables systematic lifestyle switching to take place.

At the request of the client, planners are made available to members on a dedicated website, enabling their members to undertake basic modelling on their benefits. The system calculations within the planners are tested and approved by the Administration team prior to the website becoming available to members.

<table>
<thead>
<tr>
<th>Detailed controls</th>
<th>Relevant exceptions ‘if any’</th>
<th>DB</th>
<th>DC</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.7 Member data is loaded onto the administration platform using a data validation tool. Control totals are reconciled with discrepancies investigated and escalated to the client representative, where appropriate.</td>
<td><strong>Inspection</strong>&lt;br&gt;Confirmed for a sample of clients that member data loaded onto the administration system was subject to validation and reconciliation with appropriate action taken for discrepancies.*&lt;br&gt;No exceptions to the company’s procedures were noted.</td>
<td><img src="Image1" alt="Inspection" /></td>
<td><img src="Image2" alt="No exceptions" /></td>
</tr>
<tr>
<td>1.8 For all DB schemes, a calculation specification is reviewed by the Scheme Actuary before administration go live.</td>
<td><strong>Inspection</strong>&lt;br&gt;Confirmed for a sample of new DB schemes that a calculation specification had been written and reviewed by the Scheme Actuary in advance of the scheme go live.*&lt;br&gt;No exceptions to the company’s procedures were noted.</td>
<td><img src="Image1" alt="Inspection" /></td>
<td><img src="Image2" alt="No exceptions" /></td>
</tr>
<tr>
<td>1.9 The DC scheme rules are reviewed by the Quality and Technical team to support any system developments necessary.</td>
<td>There were no DC client take-ons in this period. Therefore this control did not operate.</td>
<td><img src="Image2" alt="No exceptions" /></td>
<td><img src="Image2" alt="No exceptions" /></td>
</tr>
</tbody>
</table>

* Underlying test performed by the Reporting Accountants  
** Underlying test performed by RPMI Business Assurance team, subsequently reviewed by the Reporting Accountants.
2. Authorising and processing transactions

Contributions to defined contribution plans, defined benefit schemes, or both, and transfers of members’ funds between investment options are processed accurately and in a timely manner.

Contributions are paid in accordance with a schedule of pay cycles determined for each scheme with contributing members. The schedules include the due dates for contribution receipt and these are monitored to ensure that they are received before the 19th of the month following the members’ payroll and earlier, if rules require. The amount received is reconciled to the amount notified by the scheme sponsor. Where appropriate, delayed contribution payments are escalated to the scheme sponsor / the Pensions Regulator.

Data files are received from employers detailing contributions by employer and member. These files are uploaded onto the administration system using an automated routine which includes system validation to ensure that member data is in an appropriate format and in line with scheme rules and legislation.

Automated schedules of expected contributions are in place and a segregation exists between the Administration function processing the data files on the administration system and the Finance team entering the cash received. The reconciliation procedures are agreed with the client to ensure non-reconciling items are treated accurately and promptly.

DC contributions are allocated in accordance with member investment choices / the default investment strategy. Investment instructions are sent to the investment manager via Straight Through Processing (STP) or manually, following secondary review. Where STP is used, the Investment Manager instruction is processed via an automated gateway where the investment manager updates unit holdings and prices automatically on a daily basis. For manual processing, a contract note is received from the investment manager as confirmation of the investment instruction and details unit holdings and prices.

Transfer of members’ funds between investment options (switches) are processed following instruction from the member and are monitored in line with agreed service levels to ensure timely processing. Lifestyle strategies are designed to match target retirement age to an appropriate level of risk by managing the asset mix. Member funds are moved gradually from higher risk funds into the deposit fund over the five years to retirement. Lifestyle profiles are built into the administration system in order to enable automated lifestyle investment switches.

Regular unit reconciliations are undertaken to ensure that the units recorded by the investment manager agree to the units in the administration system, both at a member level, and in total. Any discrepancies are corrected as appropriate.
<table>
<thead>
<tr>
<th>Detailed controls</th>
<th>Relevant exceptions ‘if any’</th>
<th>DB</th>
<th>DC</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1 Contributions received are monitored and reconciled to the supporting records received from the scheme sponsor. Any differences are investigated and followed up on a timely basis.</td>
<td>Inspection Confirmed for a sample of contributions collected, that the amount received was reconciled to the supporting records received with any discrepancies investigated and appropriately resolved. No exceptions to the company’s procedures were noted.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.2 Contribution data files received from the scheme sponsor follow a sequence of automated validation steps to review integrity of member data in line with scheme rules and legislation.</td>
<td>Inspection Confirmed for a sample of contribution data files received that they were subject to automated validation. No exceptions to the company’s procedures were noted.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.3 Contributions and transfers between investment options including lifestyle switches are allocated to the correct investment products based on scheme requirements and members’ allocation requirements using automated routines. Where manual updates are made, a secondary review is carried out.</td>
<td>Observation Confirmed by walkthrough of the process, that automated routines were used to allocate the contributions / transfers to the correct investment product based on the scheme or member requirements. Inspection Confirmed for a sample of manual changes to investment options, that the investment allocation had been subject to secondary review. No exceptions to the company’s procedures were noted.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.4 Member requested DC switches; disinvestments or fund choice amendments are only processed based on member authorisation.</td>
<td>Inspection Confirmed for a sample of member changes to investment options, that member authorisation had been received. No exceptions to the company’s procedures were noted.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.5 Investment instructions provided to the investment manager are subject to secondary review. Where straight-through processing (STP) is used, investment instruction is fully automated to ensure that funds are accurately updated.</td>
<td>Inspection Confirmed for a sample of contribution investments made, that the instruction was subject to secondary review or that STP had been used. No exceptions to the company’s procedures were noted.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Benefits payable and transfer values are calculated in accordance with scheme rules and relevant legislation and are paid on a timely basis.

Automated workflows generate underlying calculation routines which are established in the administration system at the client take-on stage. Once a member case has commenced, the workflow will prompt the user at key intervals to ensure that benefits payable and transfers are processed in a timely manner and are reviewed for accuracy of input at key risk stages. Where automation is unavailable, additional checks are implemented. Updates to calculation factors are provided from an authorised source and a record is kept as a clear audit trail.

All calculations generated are subject to secondary review before they are scheduled for payment.

Reports are systematically generated to identify preserved members approaching normal retirement age. Retirement options are sent to members in order to progress the case and ensure that benefits can be paid on a timely basis.

Member details used in the calculation process such as salary, service details and AVC values are updated in the administration system using information provided from the employer to ensure that calculations are accurate.

Pensioner payroll payments are reviewed for accuracy and approved. A suite of reconciliation reports is generated highlighting a series of member movements and reconciling items. Variances from one payroll period to another are reconciled and authorised by a team leader. Any discrepancies are resolved in advance of payment. The payroll is authorised by two members of the payroll team before it is approved for payment and the BACS file is generated. A payroll checklist for each payroll is used to document the process and the reconciliations performed.

Transfers out are calculated using either automated workflows or manually using a standard process outlined in a transfer out proforma. Key documentation is required for a member to transfer out of a scheme including signed indemnity and discharge forms.

Payments initiated in the administration system are identified as part of a daily batch process and are made using BACS approved software.

### Detailed controls

<table>
<thead>
<tr>
<th>Relevant exceptions ‘if any’</th>
<th>DB</th>
<th>DC</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Underlying test performed by the Reporting Accountants</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Underlying test performed by RPMI Business Assurance team, subsequently reviewed by the Reporting Accountants.</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Underlying test performed by the Reporting Accountants
** Underlying test performed by RPMI Business Assurance team, subsequently reviewed by the Reporting Accountants.
<table>
<thead>
<tr>
<th>Detailed controls</th>
<th>Relevant exceptions ‘if any’</th>
<th>DB</th>
<th>DC</th>
</tr>
</thead>
</table>
| 2.7 Automated routines are available to calculate benefits payable and benefit estimates in accordance with scheme rules. Where manual calculations are required, they are subject to secondary review. | Inspection  
Confirmed for a sample of benefits calculated, that automated routines were used. Where this was not possible, confirmed that the manual calculation had been subject to secondary review.*  
Re-performance  
Confirmed the accuracy of the routine by undertaking a manual calculation of a benefit paid or estimate issued.*  
No exceptions to the company’s procedures were noted. |   | |
| 2.8 Factor updates are applied using client authorised sources, including government indices and Scheme Actuary notifications. | Inspection  
Confirmed for a sample of factor changes made, that the change had been appropriately authorised.*  
No exceptions to the company’s procedures were noted. |   | |
| 2.9 System generated reports identifying preserved members approaching retirement age are reviewed regularly to ensure timely communication with the member prior to normal retirement age. | Inspection  
Confirmed for a sample of members approaching normal retirement age that they had been identified within a system generated report and contacted in advance.*  
No exceptions to the company’s procedures were noted. |   | |
| 2.10 Routine benefit payments in respect of retirements are reviewed for accuracy, receipt of appropriate documentation and approved within the automated system. | Inspection  
Confirmed for a sample of members retiring from the scheme, that retirement documentation had been received and their payment had been reviewed and approved within the administration system.*  
No exceptions to the company’s procedures were noted. |   | |
| 2.11 Benefit workflows / checklists include prompts to check for AVCs and client specific factors with authorisation steps to ensure timely payment. | Inspection  
Confirmed for a sample of benefit payments, that the workflow or checklist included a prompt to check for AVCs / client specific factors and authorisation steps.*  
No exceptions to the company’s procedures were noted. |   | |

* Underlying test performed by the Reporting Accountants  
** Underlying test performed by RPMI Business Assurance team, subsequently reviewed by the Reporting Accountants.
<table>
<thead>
<tr>
<th>Detailed controls</th>
<th>Relevant exceptions ‘if any’</th>
<th>DB</th>
<th>DC</th>
</tr>
</thead>
</table>
| 2.12 Transfers are processed via automated workflows or checklists. Where automation is not available, additional secondary reviews are undertaken. | Inspection  
Confirmed for a sample of transfers, that a workflow / checklist had been used. Where manual transfers had been undertaken, confirmed that secondary checks had been undertaken.**  
No exceptions to the company’s procedures were noted. | ✏️ |    |
| 2.13 Material transfer and benefit payments meeting client-agreed criteria are subject to additional oversight. Where necessary, the case is escalated to the Scheme Actuary. | Inspection  
Confirmed for a sample of transfers or lump sum payments meeting the client criteria established that additional review had been undertaken and that the calculations had been referred to the Scheme Actuary where appropriate.**  
No exceptions to the company’s procedures were noted. | ✏️ |    |
| 2.14 An events tracker is maintained to ensure that all payrolls are identified and executed in a timely manner. | Inspection  
Confirmed that a sample of payrolls were diarised on the events tracker in accordance with client payroll cycles.**  
No exceptions to the company’s procedures were noted. | ✏️ |    |
| 2.15 During payroll processing a set suite of exception reports are generated and reviewed. This includes a review by reference to the previous month and changes in the period. Material variances are investigated with review by a senior administrator. | Inspection  
Confirmed for a sample of payrolls, that exception reports had been generated and reviewed. Confirmed that material variances had been investigated with an overall review by a senior administrator.**  
No exceptions to the company’s procedures were noted. | ✏️ |    |

* Underlying test performed by the Reporting Accountants  
** Underlying test performed by RPMI Business Assurance team, subsequently reviewed by the Reporting Accountants.
3. Maintaining financial and other records

Member records consist of up-to-date and accurate information and are updated and reconciled regularly.

We receive regular updates on member personal data from the scheme sponsors. In support of this, we carry out a series of regular data integrity checks including:

- data quality checks in line with Pensions Regulator guidance on measuring member data (‘common data’ requirements);
- member movement reconciliations;
- UK pensioner existence checks using an external tracing bureau; and
- overseas pensioner, child dependant and incapacity pensioner existence checks.

Any data discrepancies identified during these reviews are investigated. A standard protocol is followed with an established communication timeframe for the member to respond before payments are suspended until satisfactory documentation is received.

Members and scheme sponsors can update member data using a number of different methods. Standard interface files are available and can be imported into the administration system following validation checks. Member data can also be updated using the secure member website which requires a unique user log-in and password authentication.

All client communication requires authorisation from the client / member before amending member data. Member correspondence is scanned onto the document management system and filed with the member record for reference.

Benefits statements are provided to active members annually which gives them the opportunity to review personal data and raise queries with the Administration team.

<table>
<thead>
<tr>
<th>Detailed controls</th>
<th>Relevant exceptions ‘if any’</th>
<th>DB</th>
<th>DC</th>
</tr>
</thead>
</table>
| 3.1 Reports are received from an external tracing bureau to assist in UK pensioner existence reviews. All discrepancies are investigated and appropriate action taken. | Inspection
Confirmed that UK pensioner existence checks had been undertaken in the period, discrepancies investigated and action taken including suspending payments and member communication as appropriate.*
No exceptions to the company’s procedures were noted. |   |    |
| 3.2 Regular existence / case reviews are undertaken to confirm the legitimacy of certain benefit types. Receipt of certificates of existence / supporting documentation is recorded. Where necessary, member payments are suspended. | Inspection
Confirmed for a sample of pensioners residing overseas and pensions where dependants are in receipt of pension benefits, that existence checks / case reviews are carried out and supporting documentation obtained.*
No exceptions to the company’s procedures were noted. |   |    |

* Underlying test performed by the Reporting Accountants
** Underlying test performed by RPMI Business Assurance team, subsequently reviewed by the Reporting Accountants.
<table>
<thead>
<tr>
<th>Detailed controls</th>
<th>Relevant exceptions ‘if any’</th>
<th>DB</th>
<th>DC</th>
</tr>
</thead>
</table>
| 3.3 Member data is reviewed regularly to provide an accurate measurement of the quality benchmarked against the Pensions Regulator guidance, ‘Record-keeping: measuring member data’. Discrepancies are escalated to the client and appropriate action taken. | Inspection  
Confirmed for a sample of clients that member data is regularly reviewed in line with the Pensions Regulator guidance with discrepancies resolved appropriately.**  
No exceptions to the company’s procedures were noted. | | |
| 3.4 Clients provide periodic updates to member data which are uploaded onto members’ records. Exceptions are reviewed and appropriate action taken. | Observation  
Confirmed through walkthrough of the data upload procedures, that exceptions are reviewed and resolved appropriately.**  
No exceptions to the company’s procedures were noted. | | |
| 3.5 The creation of new member records and member data changes, as advised by the member or the scheme sponsor, are subject to validation checks and authorisation prior to processing on the system. | Observation  
Confirmed via walkthrough of the data upload procedures that validation checks are undertaken and authorisation is required prior to processing on the system.**  
No exceptions to the company’s procedures were noted. | | |
| 3.6 Member movement reconciliations are undertaken quarterly. Discrepancies are investigated and action taken where appropriate. Where quarterly reconciliations are not undertaken, an automated interface to the accounting system takes place. | Inspection  
Confirmed for a sample of schemes that a quarterly membership reconciliation had taken place and for a sample of discrepancies identified, reviewed action taken to confirm it was appropriate. For schemes where quarterly reconciliations are not undertaken ensured an automated interface file to the accounting system takes place.*  
No exceptions to the company’s procedures were noted. | | |
| 3.7 Individual member correspondence is scanned to a document management system which has role restricted access. Quality reviews are undertaken to ensure scanned documents are accurately filed to the respective member record. | Inspection  
Confirmed that a document management system is in operation with role restricted access.*  
Enquiry  
Confirmed by in-depth enquiry that quality reviews are undertaken to ensure scanned documents are appropriately filed.*  
No exceptions to the company’s procedures were noted. | | |
<table>
<thead>
<tr>
<th>Detailed controls</th>
<th>Relevant exceptions ‘if any’</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>3.8 Members can update and amend personal details via a secure member website.</strong></td>
<td><strong>Re-performance</strong>&lt;br&gt;Confirmed security framework for the member website through re-performance of the security logon requirements for members via the replica test website.<strong>&lt;br&gt;<strong>Inspection</strong>&lt;br&gt;Confirmed for a sample of member updates made via the website, that the changes had been accurately amended on the member record within the administration system.</strong>&lt;br&gt;<em>No exceptions to the company’s procedures were noted.</em></td>
</tr>
</tbody>
</table>

| **3.9 Member records are updated regularly via Electronic Data Interchange (EDI) using information provided by HMRC.** | **Inspection**<br>Confirmed for a sample of EDI files received from HMRC, that the member records had been accurately updated.*<br>*No exceptions to the company’s procedures were noted.* |

* Underlying test performed by the Reporting Accountants<br>** Underlying test performed by RPMI Business Assurance team, subsequently reviewed by the Reporting Accountants.
Contributions and benefit payments are completely and accurately recorded in the proper period.

Where possible, accounting journals are systematically created as part of the workflow process. A daily extract is taken from the administration system and a file is created to import into the accounting system the following day as part of the bank reconciliation process.

Where an automated solution is not suitable, a payment requisition form requires authorisation before payment and an associated journal entry in the accounting system is made. Regular bank reconciliations and cash flow forecasting identify cash transactions and a reconciliation between the administration system and the accounting system ensures that benefits processed are invoiced and recorded appropriately.

<table>
<thead>
<tr>
<th>Detailed controls</th>
<th>Relevant exceptions ‘if any’</th>
<th>DB</th>
<th>DC</th>
</tr>
</thead>
</table>
| **3.10** For schemes administered in Darlington, scheme transactions input into the pensions administration system are systematically imported into the accounting system and reconciled to bank statements daily. | Inspection
Confirmed for a sample of days, that a journal file comprising scheme transactions had been created and imported accurately into the accounting system and that a bank reconciliation had been performed.  
*No exceptions to the company’s procedures were noted.* |  |  |
| **3.11** For schemes administered in Coventry, quarterly reconciliation between the administration system and the accounting system ensures that benefits processed which have an associated charge to the employer have been accurately invoiced. | Inspection
Confirmed for a sample of schemes which have employer charges resulting from benefits processed, that a regular reconciliation had been carried out with discrepancies resolved.  
*No exceptions to the company’s procedures were noted.* |  |  |
| **3.12** Regular bank reconciliations are undertaken to ensure all cash movements are accounted for accurately in the proper period. | Inspection
Confirmed for a sample of schemes, that regular bank reconciliations had been undertaken with supporting documentation retained.  
*No exceptions to the company’s procedures were noted.* |  |  |
| **3.13** Contributions received are monitored and reconciled to the supporting records received from the scheme sponsor. Any differences are investigated and followed up on a timely basis. | Inspection
Confirmed for a sample of contributions collected, that the amount received was reconciled to the supporting records received with any discrepancies investigated and appropriately resolved.  
*No exceptions to the company’s procedures were noted.* |  |  |

* Underlying test performed by the Reporting Accountants
** Underlying test performed by RPMI Business Assurance team, subsequently reviewed by the Reporting Accountants.
**Investment transactions, balances and related income are completely and accurately recorded in the proper period.**

The administration system uses a routine to upload contribution files received, referencing each member investment allocation weights and aggregating the nominal investment amount for each fund. The investment instruction (automated where possible) is then sent to the Investment Manager using the aggregate investment data. Unit reconciliations are carried out to confirm that the units held by the Investment Manager agree to the units held on the member’s record in the administration system. System generated unit data reports are compared to the Investment Manager statements, both at the member level and the fund(s) in aggregate. Discrepancies of more than one unit are fully investigated and resolved with the manager.

Regular bank reconciliations ensure that all investment related income is identified and recorded appropriately on the date it is received.

We ensure that cash transactions in respect of fund manager subscriptions and redemptions are suitably authorised and that where required, the custodian has been duly informed. We receive regular reports from the custodian to ensure that the cash transactions processed reconcile to their records.

Investment purchases, sales and valuation information are received from the investment manager, custodian or outsourced investment accountant and reconciled for the audited year end scheme accounts.

<table>
<thead>
<tr>
<th>Detailed controls</th>
<th>Relevant exceptions ‘if any’</th>
<th>DB</th>
<th>DC</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.14 Regular unit reconciliations ensure that the units held by the Investment Manager correspond to the units recorded in the pensions administration system at member and fund level.</td>
<td>Inspection&lt;br&gt;Confirmed for a sample of schemes, that unit reconciliations are carried out between the units stated by the investment manager and those recorded in the pensions administration system.**&lt;br&gt;No exceptions to the company’s procedures were noted.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.15 Investment transactions are identified and accounted for as part of the bank reconciliation, which is subject to review by a senior accountant.</td>
<td>Inspection&lt;br&gt;Confirmed that regular bank reconciliations had been undertaken and reviewed by a senior accountant.*&lt;br&gt;No exceptions to the company’s procedures were noted.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.16 Investment instructions provided to the investment manager are subject to secondary review. Where straight-through processing (STP) is used, investment instruction is fully automated to ensure that funds are accurately updated.</td>
<td>Inspection&lt;br&gt;Confirmed for a sample of contribution investments made, that the instruction was subject to secondary review or that STP had been used.**&lt;br&gt;No exceptions to the company’s procedures were noted.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Scheme documents (deeds, policies, contracts, booklets) are complete, up to date and securely held.**

Scheme documentation including policies, contracts and guides to services are retained securely in document management systems with appropriate access restrictions and version control.

Where RPMI is responsible for maintaining original scheme documents, consultation with scheme actuaries and legal advisors is integral in ensuring all scheme documentation including valuation statements, schedules of contributions and trust deeds are both accurate and complete.

To make certain that all administrative tasks are undertaken in the event of a change to scheme rules, a checklist is used by the Technical team to ensure the accurate and timely execution of the trust deed.

Our secure member website provides access to scheme booklets. The area is secured requiring members to enter a unique username and password.

<table>
<thead>
<tr>
<th>Detailed controls</th>
<th>Relevant exceptions ‘if any’</th>
<th>DB</th>
<th>DC</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.17 Scheme information, policies and contracts are held in an electronic document management system which is subject to access and version control.</td>
<td>Inspection Confirmed for a sample of scheme information maintained in the document management system, that access and version control was in place and appropriate.** No exceptions to the company’s procedures were noted.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.18 A secure member area within the RPMI website is available to clients which enables members to view an online version of their scheme booklet and a library of other relevant documentation.</td>
<td>Inspection Confirmed for a sample of schemes that the current scheme booklet was available on the website and reviewed the security configuration supporting the member area to ensure this was adequate.** No exceptions to the company’s procedures were noted.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.19 At the request of the Trustee, electronic deeds are stored in a document management system in addition to hard copies retained in a secure location.</td>
<td>Inspection Confirmed for a sample of deeds executed, that an electronic copy is available on the document management system in addition to hard copy stored in a secured location.** No exceptions to the company’s procedures were noted.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.20 A deed chart is maintained to monitor the progress of a deed through to execution.</td>
<td>Inspection Confirmed the existence of the deed chart. Confirmed via inspection of the chart, that this was regularly maintained.** No exceptions to the company’s procedures were noted.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Detailed controls | Relevant exceptions ‘if any’ | DB | DC
---|---|---|---
3.21 Scheme booklets are monitored to provide version control and ensure that the correct booklets and supporting items are included in the new entrant pack. | **Inspection**
Confirmed that monitoring of scheme booklets took place through review of the scheme booklet schedule maintained.**
No exceptions to the company’s procedures were noted. |  |  |

### 4. Safeguarding assets

**Member and scheme data is appropriately stored to ensure security and protection from unauthorised use.**

Access to the network is restricted via a robust network domain policy which enforces complex password setting in accordance with ISO 27001 Information Security Standard. (Please see section 7 within IT for further details).

At the application level, access is restricted on a client / scheme basis commensurate to users’ involvement with the scheme. Access permissions are managed by the dedicated IT service desk and require management authorisation. There are several layers of user permissions within the administration applications which are restricted on a role basis.

Member correspondence, both incoming and outgoing, is scanned onto the respective member record within the administration application. Quality reviews are undertaken to ensure the data is loaded to the correct member record. All hard copy data is retained in secured storage overnight; this is governed by the Clear Desk Policy. The policy is documented in the Computer Users Handbook which is available to all employees on the RPMI intranet.

All clients are offered encryption tools which provide additional security layers when transferring data over email transmissions. Passwords are used where encryption has not been deployed.

#### Detailed controls

<table>
<thead>
<tr>
<th>Detailed controls</th>
<th>Relevant exceptions ‘if any’</th>
<th>DB</th>
<th>DC</th>
</tr>
</thead>
</table>
| **4.1** Enforced password security protocols are in place requiring users to adopt minimum complex character length with regular change requirements. | **Inspection**
Confirmed via inspection of the network configuration that enforced password requirements were in place.**
No exceptions to the company’s procedures were noted. |  |  |

* Underlying test performed by the Reporting Accountants
** Underlying test performed by RPMI Business Assurance team, subsequently reviewed by the Reporting Accountants.
Cash is safeguarded and payments are suitably authorised and controlled.

All clients operate a separate bank account which initially requires Trustee signed mandate approval. Internal authorised signatories are set for each of the bank accounts, with two signatories necessary to make any changes to the bank mandate.

Payments created within the administration system enforce dual authorisation with only specific permitted roles enabled to process payments. Administrators creating the payments do not have access to any of the banking systems, including BACS, internet banking, CHAPs or cheques. The banking systems are further configured to require dual authorisation, with an authentication token adding a further layer of security.

Pensioner payrolls are reconciled each period and the reconciliation pack is reviewed by a senior member of the team. The payroll reporting pack includes a series of exception reports designed to identify any high value / unusual transactions. Each exception identified is subject to investigation and client specific payroll tolerances are set to ensure appropriate oversight.

Cash forecasting is undertaken at a frequency deemed proportionate with the client. Cash sweeping arrangements are applied, where appropriate, to ensure appropriate cash levels are maintained. This process is supported by the routine bank reconciliation which has senior oversight ensuring that unreconciled items are fully investigated and accounted for.
<table>
<thead>
<tr>
<th>Detailed controls</th>
<th>Relevant exceptions ‘if any’</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>4.5</strong> Each new scheme bank account requires Trustee signed approval.</td>
<td><strong>Inspection</strong> Confirmed for a sample of new bank accounts, that new bank account mandates are signed by the Trustee and supported by Trustee resolution. Confirmed that changes to bank account mandates are authorised by two existing signatories with appropriate authority levels.*&lt;br&gt;No exceptions to the company’s procedures were noted.</td>
</tr>
<tr>
<td>Changes to mandates require two RPMI authorised signatories.</td>
<td></td>
</tr>
<tr>
<td><strong>4.6</strong> Segregations exist ensuring those initiating benefit payments differ from</td>
<td><strong>Inspection</strong> Confirmed for a sample of benefit payments, that a segregation of duties exists between those initiating and processing benefit payments.**&lt;br&gt;No exceptions to the company’s procedures were noted.</td>
</tr>
<tr>
<td>those processing the payments. All payments created in the administration system require secondary authorisation.</td>
<td></td>
</tr>
<tr>
<td><strong>4.7</strong> Access to the BACS application is restricted via unique user sign in and</td>
<td><strong>Observation</strong> Confirmed via walkthrough of the BACS payments process, that access to the BACS application is restricted via unique user sign in and authentication card.<strong>&lt;br&gt;<strong>Inspection</strong> Confirmed for a sample of payrolls, that reconciliations had taken place to ensure payments identified by the administration system agreed to the BACS reports generated.</strong>&lt;br&gt;No exceptions to the company’s procedures were noted.</td>
</tr>
<tr>
<td>authentication card. A reconciliation is carried out to verify that the BACS submission agrees to the internal payment processing system.</td>
<td></td>
</tr>
<tr>
<td><strong>4.8</strong> Regular bank reconciliations are carried out and are subject to senior</td>
<td><strong>Inspection</strong> Confirmed that regular bank reconciliations had been undertaken with supporting documentation retained.*&lt;br&gt;No exceptions to the company’s procedures were noted.</td>
</tr>
<tr>
<td>review. Reconciling items identified are investigated and action taken where</td>
<td></td>
</tr>
<tr>
<td>appropriate.</td>
<td></td>
</tr>
</tbody>
</table>

* Underlying test performed by the Reporting Accountants  
** Underlying test performed by RPMI Business Assurance team, subsequently reviewed by the Reporting Accountants.
5. Monitoring compliance

Contributions are received in accordance with scheme rules and relevant legislation.

Payroll schedules are maintained to ensure that contributions are received in line with payroll cycles and relevant legislation and that late contributions can be escalated to the scheme sponsor for resolution. When contribution income is received, a member of the Finance team updates the schedule with the date of receipt.

At the client request, RPMI will invoice employers for their contribution liability using proprietary software. The software is updated using the Schedule of Contributions and referencing the administration system to ensure the contribution rates and any recovery payments are calculated accurately for the membership within the period.

A register of future changes to contributions outlined in the Schedule of Contributions is maintained by the Technical team to ensure updates to the relevant systems are made accurately. Changes to the contribution rates within the administration system require authorisation within the Administration function with restricted access to Group IT for implementation. Daily exception reports are generated and reviewed to ensure any changes to contributions within the system have been made in accordance with the Schedule of Contributions and appropriately authorised.

Schedules are maintained for the receipt of the contributions and escalation reporting for late / nil receipt is established to the scheme sponsor / Pensions Regulator in accordance with the Regulator’s requirements.

* Underlying test performed by the Reporting Accountants
** Underlying test performed by RPMI Business Assurance team, subsequently reviewed by the Reporting Accountants.
<table>
<thead>
<tr>
<th>Detailed controls</th>
<th>Relevant exceptions ‘if any’</th>
</tr>
</thead>
</table>
| **5.1** Receipt of contributions is monitored against client-approved schedules so that incorrect or late contributions can be identified and follow-up action taken. | Inspection  
Confirmed for a sample of contributions collected, that the amount received was reconciled to the supporting records received with any discrepancies investigated and appropriately resolved.**  
No exceptions to the company’s procedures were noted. |
| **5.2** Where requested by the client, contribution rates authorised by the Trustee are recorded in the administration system and systematically referenced for employer contribution invoicing. | Inspection  
Confirmed for a sample of schemes, that the contribution rate approved by the Trustee reconciled to the rate recorded in the administration system and that used for the employer contributions invoicing.*  
No exceptions to the company’s procedures were noted. |
| **5.3** Changes to contribution rates within the administration system are appropriately authorised and subject to daily review. | Inspection  
Confirmed for a sample of contributions rate changes, that they had been appropriately authorised and that the rates were reviewed daily.*  
No exceptions to the company’s procedures were noted. |
| **5.4** A register of schemes is maintained to record future contribution rate changes to enable the timely update of the administration system. | Inspection  
Confirmed the existence of the register and for a sample of schemes listed, reviewed the current and future rates listed to ensure they agreed to the Trustee approved rate.*  
No exceptions to the company’s procedures were noted. |

* Underlying test performed by the Reporting Accountants
** Underlying test performed by RPMI Business Assurance team, subsequently reviewed by the Reporting Accountants.
### Detailed controls

#### 5.5 Receipt of contributions is monitored in line with The Pension Regulator’s requirements and relevant legislation. Late contributions are reported to the scheme sponsor / Pensions Regulator as appropriate.

<table>
<thead>
<tr>
<th>Relevant exceptions ‘if any’</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Inspection</strong></td>
</tr>
<tr>
<td>Confirmed for a sample of months that any instances of late receipt of contributions were reported to the scheme sponsor / Pensions Regulator as appropriate.**</td>
</tr>
<tr>
<td><strong>No exceptions to the company’s procedures were noted.</strong></td>
</tr>
</tbody>
</table>

#### 5.6 Contribution data follows a sequence of validation steps which mirror the scheme rules and relevant legislation prior to import into the pension administration database.

<table>
<thead>
<tr>
<th>Relevant exceptions ‘if any’</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Inspection</strong></td>
</tr>
<tr>
<td>Confirmed for a sample of contribution data files received that they were subject to automated validation.**</td>
</tr>
<tr>
<td><strong>No exceptions to the company’s procedures were noted.</strong></td>
</tr>
</tbody>
</table>

---

**Services provided to pension schemes are in line with service level agreements.**

Overseeing the full service provision are the Client Relationship Managers (CRM). The CRM is the first point of contact for the client and regularly liaises with the Administration team to discuss service provisions.

Casework management is reviewed daily. All incoming mail is reviewed, logged and tracked against the respective service level. Team managers delegate the incoming work on a daily basis and receive updates from the administrators on work outstanding / in progress. A weekly case review meeting with senior management considers performance management and resource capacity further.

To assist in the service oversight, workflows within the administration system are configured with pre-defined time capture stages, ensuring the integrity of performance reporting.

Appropriate training is provided to administrators with training records maintained. Only administrators trained on a particular process are permitted to administer the case.

---

### Detailed controls

#### 5.7 Team managers allocate incoming casework and review existing workloads daily to ensure that service levels can be prioritised and casework is carried out by administrators who have the appropriate training.

<table>
<thead>
<tr>
<th>Relevant exceptions ‘if any’</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enquiry</strong></td>
</tr>
<tr>
<td>Confirmed via discussion with team managers that incoming casework and workload are reviewed daily to ensure appropriate allocation and prioritisation of service levels.**</td>
</tr>
<tr>
<td><strong>No exceptions to the company’s procedures were noted.</strong></td>
</tr>
</tbody>
</table>

#### 5.8 Regular training is provided to all staff as appropriate to ensure their knowledge of administration processes and relevant legislation is up to date.

<table>
<thead>
<tr>
<th>Relevant exceptions ‘if any’</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Inspection</strong></td>
</tr>
<tr>
<td>Confirmed for a sample of pension administrators that training records were maintained.*</td>
</tr>
<tr>
<td><strong>No exceptions to the company’s procedures were noted.</strong></td>
</tr>
</tbody>
</table>

---

* Underlying test performed by the Reporting Accountants

** Underlying test performed by RPMI Business Assurance team, subsequently reviewed by the Reporting Accountants.
5.9 Casework monitored by workflows have inbuilt time captures at key event stages to enable performance targets to be measured accurately.

Inspection
Confirmed via inspection of the system configuration that a sample of workflows have inbuilt time captures at key stage events to enable accurate performance measurements.*

No exceptions to the company’s procedures were noted.

5.10 Performance against service levels is reported to senior management to consider resource allocation and workload.

Inspection
Confirmed for a sample of months that performance against service levels are being reported and considered by senior management.*

No exceptions to the company’s procedures were noted.

Transaction errors are rectified promptly and clients treated fairly.

A standard procedure is in place to ensure that complaints are handled effectively and escalated appropriately. A schedule is maintained to log the current status of each complaint and record the eventual outcome. Schedules are overseen by senior administrators who will act as direct liaison for the member and RPMI.

Overseeing the complaint and error process is the Breach Management Group, comprising senior management. The Group reviews the Errors and Omissions database used to record and track errors. The Group’s remit is to undertake root cause analysis to identify and implement any remedial action necessary.

5.11 Documented procedures are in place to manage complaints. Schedules are maintained to monitor the progress of complaints; oversight of this is assigned to trained administrators. Members receive regular progress updates.

Inspection
Confirmed that complaint procedures are documented and that complaints schedules are maintained to monitor the progress of action taken.**

No exceptions to the company’s procedures were noted.

5.12 An Errors and Omissions database is maintained to record and track errors and omissions. Scheme sponsors are notified as appropriate. Remedial action is undertaken promptly and overseen by the Breach Management Group.

Inspection
Confirmed through inspection of the database, that errors and omissions are recorded and progress of action taken is monitored.**

No exceptions to the company’s procedures were noted.

* Underlying test performed by the Reporting Accountants
** Underlying test performed by RPMI Business Assurance team, subsequently reviewed by the Reporting Accountants.
6. Reporting to clients

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

Quarterly reports are prepared in accordance with clients’ requirements using bespoke templates. The preparation of the reports is scheduled on client-specific event trackers, which act as an online diary system for the Administration team, and each report is fully reviewed against source data extracts before submission to the client.

The Annual Benefit Statement production is scheduled on client-specific event planners to ensure statutory deadlines and client elections are met. Routines within the administration system provide the underlying calculations; these are tested before use in the live environment and validation routines take place ensuring that any anomalies in the production are identified and rectified before member distribution.

<table>
<thead>
<tr>
<th>Detailed controls</th>
<th>Relevant exceptions ‘if any’</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1 An administration timetable is maintained to ensure the timely distribution of client reports and Annual Benefit Statements.</td>
<td>Inspection Confirmed for a sample of periods, that the client reports and Annual Benefit Statements were included on the administration timetable.** No exceptions to the company’s procedures were noted.</td>
</tr>
<tr>
<td>6.2 Quarterly client reports are prepared and reviewed for accuracy and completeness before distributing to the client.</td>
<td>Inspection Confirmed for a sample of client reports, that they had been reviewed for accuracy before distribution.* No exceptions to the company’s procedures were noted.</td>
</tr>
<tr>
<td>6.3 System routines are used to generate Annual Benefit Statements. Testing is undertaken to ensure accuracy before the statements are issued to members.</td>
<td>Inspection Confirmed for a sample of Annual Benefit Statements run, that testing had been undertaken to ensure the accuracy of the statement before issuing to members.* No exceptions to the company’s procedures were noted.</td>
</tr>
</tbody>
</table>

Annual Reports and Accounts are prepared in accordance with applicable law and regulations.

Annual Report and Accounts are prepared promptly after the scheme year end. Internal planners are in place to ensure that the necessary resource is available and there is early engagement with the external audit team to coordinate a timetable for all relevant parties, ensuring that statutory deadlines are met. Accounts are prepared in accordance with the Statement of Recommended Practice and the draft reports are reviewed before issue to the client / scheme auditor.

Analytical reviews are carried out and overseen by a senior accountant, ensuring that material variances are identified and resolved regularly throughout the year.

* Underlying test performed by the Reporting Accountants
** Underlying test performed by RPMI Business Assurance team, subsequently reviewed by the Reporting Accountants.
6.4 A timetable for the preparation of the Annual Report and Accounts is established in consultation with scheme auditors.

- **Inspection**
  Confirmed for a sample of schemes that a timetable for the preparation of the Annual Report and Accounts is established in consultation with scheme auditors.**

- **No exceptions to the company’s procedures were noted.**

6.5 Analytical reviews are undertaken periodically throughout the year and investigated as necessary. These are reviewed by a senior accountant.

- **Inspection**
  Confirmed for a sample of schemes, that analytical reviews were undertaken throughout the year and the results reviewed by a senior accountant.**

- **No exceptions to the company’s procedures were noted.**

6.6 Annual Report and Accounts are prepared in accordance with the latest Statement of Recommended Practice. Draft accounts are quality checked before issue to the scheme auditor.

- **Inspection**
  Confirmed for a sample of schemes, that annual Report and Accounts are prepared in accordance with the latest Statement of Recommended Practice.**

- Confirmed that accounts are peer reviewed prior to issue to the scheme auditor.**

- **No exceptions to the company’s procedures were noted.**

### Regulatory reports are made if necessary

Corporate policies are in place to ensure employees are aware of their responsibilities for whistleblowing, and monitoring to prevent money laundering and bribery. The policies are provided upon induction with periodic refresher training provided. The policies are made available on the company intranet.

The Technical team monitors regulatory and legislative developments in the pensions environment, providing appropriate updates to colleagues via intranet articles and training sessions.

The Pension Scheme Return and Annual HMRC Events Report are completed using a series of data extract routines to ensure accuracy and completeness of the submissions. A log is maintained to record potential Pensions Regulator notifiable events. The log is reviewed by the in-house Technical team to determine if there is a reporting requirement. Where appropriate, the matter is escalated to the Pensions Policy team, made up of qualified actuaries, to provide additional expertise and oversight.

Where necessary, Action Fraud is notified where due diligence criteria for a transferring scheme has not been met to assist in the prevention of Pension Liberation Fraud.

---

* Underlying test performed by the Reporting Accountants

** Underlying test performed by RPMI Business Assurance team, subsequently reviewed by the Reporting Accountants.
<table>
<thead>
<tr>
<th>Detailed controls</th>
<th>Relevant exceptions ‘if any’</th>
<th>DB</th>
<th>DC</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.7 All employees, as part of the induction process, receive training on anti-money laundering and whistleblowing. The policies are available on the company intranet.</td>
<td><strong>Inspection</strong> Confirmed for sample of employees that they had received training on the anti-money laundering and whistleblowing procedures as part of the induction process.** Confirmed that the anti-money laundering and whistleblowing policies are available on the intranet.** No exceptions to the company’s procedures were noted.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.8 The Technical team monitors regulatory and legislative developments for any potential changes to the pension environment and changes to reporting requirements. Technical updates are available to all staff via the intranet.</td>
<td><strong>Inspection</strong> Confirmed via inspection of the intranet that regular technical updates were made available.* No exceptions to the company’s procedures were noted.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.9 Data extract routines are in place to capture reportable events and enable the Pension Scheme Event Return and Annual HMRC Events Report to be completed and submitted within the required timescales. HMRC reports are completed for all overseas transfers.</td>
<td><strong>Inspection</strong> Confirmed via inspection of the data capture routines and verified the results to the annual HMRC event report.* Confirmed for a sample of overseas transfers that a necessary HMRC report had been completed.* No exceptions to the company’s procedures were noted.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.10 A Notifiable Events log is reviewed by the Technical team to assess the reporting requirement to the Pension Regulator. Where necessary, the Pensions Policy team will review the event and confirm if any reporting requirement is necessary.</td>
<td><strong>Inspection</strong> Confirmed via inspection that a notifiable events log was maintained and for a sample of events which were recorded as notifiable, obtained the communication provided to the Pensions Regulator.* No exceptions to the company’s procedures were noted.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.11 Procedures exist to ensure appropriate due diligence is carried out on suspected Pension Liberation Fraud schemes. The procedures identify the requirements for reporting to the Pensions Regulator / Action Fraud helpline.</td>
<td><strong>Inspection</strong> Confirmed via inspection of the Pension Liberation Fraud procedures that escalation reporting requirements to the Pensions Regulator and Action Fraud helpline are included.** No exceptions to the company’s procedures were noted.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Underlying test performed by the Reporting Accountants
** Underlying test performed by RPMI Business Assurance team, subsequently reviewed by the Reporting Accountants.
## 7. Restricting access to systems and data

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

Access to RPMI offices is restricted to authorised personnel by an automated access entry system. The Darlington office operates continual closed circuit television (CCTV) cameras and security guards 24 hours a day, 365 days per year. Access to sensitive areas of the premises, including the IT infrastructure rooms, is limited to authorised personnel. Supporting the internal production sites in Darlington and Coventry, our virtual server environment is maintained in an offsite data centre which is ISO 27001 accredited.

In accordance with our Computer User Handbook, employees must ensure that visitors are met at reception and adhere to our visitor procedures.

<table>
<thead>
<tr>
<th>Detailed controls</th>
<th>Relevant exceptions ‘if any’</th>
</tr>
</thead>
</table>
| **7.1 Access to our premises is restricted to authorised individuals via an automated access system.** | **Inspection**
Confirmed via physical inspection that an automated access entry system is in operation in Coventry and Darlington.**
No exceptions to the company’s procedures were noted. |
| **7.2 The Darlington office operates 24/7 CCTV.** | **Observation**
Confirmed that the Darlington office operates CCTV.*
| **Enquiry**
Confirmed via discussion with security personnel that CCTV is monitored 24/7.*
No exceptions to the company’s procedures were noted. |
| **7.3 All visitors must register their details at reception. Employees are aware of the visitor procedure as outlined in the Computer User Handbook.** | **Inspection**
Confirmed via inspection of the visitor log, that visitors registered their details.*
Reviewed the Computer User Handbook to confirm that visitor procedures are in place.*
No exceptions to the company’s procedures were noted. |
| **7.4 Access to sensitive areas of the business, including critical IT infrastructure, are restricted to authorised personnel only.** | **Inspection**
Confirmed via physical inspection that the sensitive areas of the business, including critical IT infrastructure, could not be accessed by unauthorised personnel.*
No exceptions to the company’s procedures were noted. |
<table>
<thead>
<tr>
<th>Detailed controls</th>
<th>Relevant exceptions ‘if any’</th>
</tr>
</thead>
</table>
| **7.5** The offsite datacentre which is ISO 27001 accredited has the following security measures in place: 24/7 security monitoring, CCTV, electronic key access and security alarm. | **Inspection**<br>Confirmed via inspection of the accreditation certificate that the data centre is ISO 27001 Information Security accredited.*  
**Enquiry**<br>Confirmed via enquiries made with the data centre representatives that no changes to the IT security environment had taken place.*  
No exceptions to the company's procedures were noted. |
Logical access to computer systems, programs, master data, transaction data and parameters, including access by administrators to applications, databases, systems and networks, is restricted to authorised individuals via information security tools and techniques.

All RPMI policies are outlined in our Computer User Handbook which is given to all new employees upon induction, with refresher awareness sessions carried out for all employees on a regular basis. The Handbook is made available on the intranet and is updated to reflect changes in practices when necessary. All employees must sign to agree to any changes or updates to the Handbook.

User profiles are defined by relevant senior management and set up by Group IT during the employee induction process. Employees are only provided with access to applications appropriate to their function and at a level commensurate with their role and responsibility. Subsequent changes to user access must be formally requested through an electronic request system and authorised by the line manager. The changes are then implemented by the Group IT team.

We adopt a robust network domain policy which ensures staff change their password every 30 days and set a minimum complex password of at least eight characters. Three failed attempts into the network will result in the user account locking. Unauthorised access to company systems is prevented through the use of user login IDs and passwords.

We restrict administrator permissions within the network and to key applications to authorised members within Group IT and access is monitored.

Only authorised personnel are provided with remote working facilities. Our policy on mobile devices, such as mobile phones, outlines users’ responsibilities and acceptable usage. Passwords are applied to all devices and the network is configured to enable remote wiping of data if required. Authentication is required to access the network remotely.

### Detailed controls

<table>
<thead>
<tr>
<th></th>
<th>Relevant exceptions ‘if any’</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6</td>
<td>A Computer User Handbook is in place that outlines the responsibilities which all employees must adhere to with regards to information security and IT protocols. The policy is made available on the company intranet.</td>
</tr>
<tr>
<td>Inspection</td>
<td>Confirmed via inspection of the Computer User Handbook that it outlines employees’ responsibilities with regards to information security and IT protocols. Reviewed the intranet and confirmed the up-to-date Computer User Handbook was available.*</td>
</tr>
<tr>
<td>No exceptions to the company’s procedures were noted.</td>
<td></td>
</tr>
<tr>
<td>7.7</td>
<td>Enforced password security protocols are in place requiring users to adopt minimum complex character length with regular change requirements.</td>
</tr>
<tr>
<td>Inspection</td>
<td>Confirmed via inspection of the network configuration that enforced password requirements were in place.*</td>
</tr>
<tr>
<td>No exceptions to the company’s procedures were noted.</td>
<td></td>
</tr>
<tr>
<td>7.8</td>
<td>Password protected screen savers operate on all PCs and laptops connected to the network following a period of inactivity.</td>
</tr>
<tr>
<td>Inspection</td>
<td>Confirmed via inspection of network configuration settings that password protected screen savers operate on all PCs and laptops connected to the network.**</td>
</tr>
<tr>
<td>No exceptions to the company’s procedures were noted.</td>
<td></td>
</tr>
</tbody>
</table>

* Underlying test performed by the Reporting Accountants
** Underlying test performed by RPMI Business Assurance team, subsequently reviewed by the Reporting Accountants.
<table>
<thead>
<tr>
<th>Detailed controls</th>
<th>Relevant exceptions ‘if any’</th>
</tr>
</thead>
</table>
| 7.9  Access requirements are determined upon appointment and are authorised by an appropriate senior officer. | **Inspection**  
Confirmed for a sample of new users, that the level of access to the various applications and systems was commensurate to their role and had been approved by an appropriate senior officer.**  
No exceptions to the company’s procedures were noted. |
| 7.10 All new users or changes to user access require senior authorisation.        | **Inspection**  
Confirmed for a sample of access changes, that the change had been appropriately authorised.**  
No exceptions to the company’s procedures were noted. |
| 7.11 Network user accounts can be created and modified by Group IT only.         | **Inspection**  
Confirmed via inspection of the network security settings that user account creation and modification is restricted to Group IT.**  
No exceptions to the company’s procedures were noted. |
| 7.12 For leaving employees, a checklist is completed that includes a step to notify IT to disable the user profile. | **Inspection**  
Confirmed for a sample of employees who left RPMI, that a checklist had been completed.*  
No exceptions to the company’s procedures were noted. |
| 7.13 Remote access requires a certified, encrypted device with unique login details or two factor authentication to access the network. | **Re-performance**  
Confirmed via accessing the network remotely that a certified device or two factor authentication was required.**  
No exceptions to the company’s procedures were noted. |
| 7.14 Administrator access to systems is restricted to authorised individuals.   | **Inspection**  
Confirmed via inspection of administrator access rights within a sample of systems that those listed were appropriate given their role.**  
No exceptions to the company’s procedures were noted. |
| 7.15 Data can be deleted from mobile devices remotely, in the event of theft or loss. | **Inspection**  
Confirmed via review of the system configuration, that mobile devices could be remotely wiped in the event of theft or loss.**  
No exceptions to the company’s procedures were noted. |
Segregation of incompatible duties is defined, implemented and enforced by logical security controls in accordance with job roles.

Our key systems, including the Administration and Finance systems, have logical configuration established to ensure that enforced segregations are in place for key processes. The systems have different user profiles available to ensure that only necessary access is granted and management review user access regularly to ensure it remains appropriate to users’ roles.

Formal requests are necessary to grant employees, temporary employees and consultants access to the network and applications as required. Requests are made through an electronic request system or by completion of an access request form. Upon receipt of a request, the IT Operations team will create an appropriate user ID.

A list is maintained of personnel authorised to request access changes for users. Authorised managers request modifications to application access to reflect employee terminations, transfers or changes in functional responsibilities. Upon receipt of a valid request from an authorised manager, the IT Operations team will modify or terminate the relevant ID.

<table>
<thead>
<tr>
<th>Detailed controls</th>
<th>Relevant exceptions ‘if any’</th>
</tr>
</thead>
</table>
| **7.16** Administrator access to systems is restricted to authorised individuals. | Inspection  
Confirmed via inspection of user profile accounts, that administrator access to systems is restricted to authorised personnel.**  
No exceptions to the company’s procedures were noted. |
| **7.17** User profiles are created for each system and role to enforce appropriate segregation of duties. | Inspection  
Confirmed via inspection of user profile accounts, that Group IT maintained the Administrator permissions and that profiles were particular to each user.**  
No exceptions to the company’s procedures were noted. |
| **7.18** User access privileges are reviewed by line management on a regular basis. | Inspection  
Confirmed user access reviews had been completed and, for a sample of changes identified, access privileges had been amended accordingly.**  
No exceptions to the company’s procedures were noted. |
| **7.19** User profiles can only be created by an authorised individual and senior approval is required before implementation. | Inspection  
Confirmed for a sample of user profile accounts, that the user profile was created by Group IT and was appropriately authorised.**  
No exceptions to the company’s procedures were noted. |

* Underlying test performed by the Reporting Accountants  
** Underlying test performed by RPMI Business Assurance team, subsequently reviewed by the Reporting Accountants.
8. Providing integrity and resilience to the information processing environment, commensurate with the value of the information held, information processing performed and external threats

IT processing is authorised and scheduled appropriately and exceptions are identified and resolved in a timely manner.

Our Group IT team provides 24-hour business support through the monitoring of servers, local area networks, external communications and critical applications.

Segregations exist such that any changes to live systems must be authorised by the appropriate member of staff. A list of authorised personnel particular to each system/application is maintained.

IT processes are listed in annual plans and daily checklists enabling key IT processes to be scheduled effectively. Written procedures are in place for IT processing and monitoring.

Scheduled processes are monitored by Group IT and these are signed for upon completion. Any processing issues and errors are reviewed by Group IT and appropriate follow-up actions taken.

<table>
<thead>
<tr>
<th>Detailed controls</th>
<th>Relevant exceptions ‘if any’</th>
</tr>
</thead>
</table>
| 8.1 Changes to systems can only be made by authorised staff. | Inspection  
Confirmed that for a sample of changes made, the employee approving the change was a designated authority.**  
No exceptions to the company’s procedures were noted. |
| 8.2 All scheduled IT processes are documented, appropriately monitored and reviewed upon completion. Daily IT schedules operate to ensure IT processing and these are reviewed to ensure accuracy and completeness. | Inspection  
Confirmed from a sample of days, that the scheduled IT processes had been documented and reviewed upon completion.**  
Exception  
For one day from the sample selected, a series of scheduled IT processes had not been signed off to confirm that they had been completed. Further inspection confirmed that, due to the underlying automated processes, the scheduled tasks had been successfully completed.  
Management Response  
Group IT employees have been reminded of the importance of maintaining evidence that processes are complete. Following further enquiry and inspection, we were able to confirm that all scheduled tasks had been completed and there were no issues arising. |

Data transmissions between the service organisation and its counterparties are complete, accurate, timely and secure.

Encryption solutions are available for sensitive data transmitted via email. Where encryption solutions are not utilised, emails containing sensitive data are password protected. Additionally, clients are also offered File Transfer Protocol (FTP) and Secure File Transfer Protocol (SFTP) for file transfers.
We have standard interface files which enable counterparties to send information in a secure, consistent format to enable efficient and accurate upload and maintenance of the data held. A schedule exists to ensure that we remain aware of when files are expected. We will escalate to the appropriate client representative in the event that the files are not received.

We appreciate the importance of data security and aim to embed this throughout the organisation through training seminars which are underpinned by various policies, including our password and IT security policy. Our aim is to improve employee awareness and to prevent the loss or compromise of data.

A key data transfer which we undertake daily involves the BACS file transmission used to send member and supplier payments. We use only approved BACS software for sending BACS files. The software not only provides the security required but has inbuilt integrity checks to ensure the data format is acceptable.

<table>
<thead>
<tr>
<th>Detailed controls</th>
<th>Relevant exceptions ‘if any’</th>
</tr>
</thead>
</table>
| 8.3 File transfer protocol (FTP) and Secure File transfer protocol (SFTP) is available for transmitting data to external parties. | Observation
Observed the sending of a data file via FTP / SFTP.*
No exceptions to the company’s procedures were noted. |
| 8.4 Sensitive data transmitted via email is encrypted or password protected. A data security policy which outlines the rules on data transmissions is provided to all employees. | Inspection
Confirmed for a sample of external parties participating in auto-encryption that the necessary configuration has been established to ensure data transmissions are in accordance with the agreed encryption method. Obtained the data security policy and confirmed this incorporated data transmission protocols.*
No exceptions to the company’s procedures were noted. |
| 8.5 Standard interface files are available to employers to communicate member information. A schedule of expected files is maintained and regularly monitored. Any discrepancies are investigated. | Inspection
Confirmed that a schedule of expected interface files is maintained and where discrepancies arose, appropriate action was taken.*
No exceptions to the company’s procedures were noted. |
| 8.6 Data security protocols form part of regular IT training provided to employees. | Inspection
Confirmed via inspection of the training materials that data security training is carried out with employees periodically.**
No exceptions to the company’s procedures were noted. |
| 8.7 BACS approved software is used for processing transactions. | Inspection
Confirmed by review of the BACS approved software suppliers list, that software used by RPMI is approved by BACS.**
No exceptions to the company’s procedures were noted. |

* Underlying test performed by the Reporting Accountants
** Underlying test performed by RPMI Business Assurance team, subsequently reviewed by the Reporting Accountants.
**Underlying test performed by the Reporting Accountants**

**Underlying test performed by RPMI Business Assurance team, subsequently reviewed by the Reporting Accountants.**

---

**Detailed controls**

<table>
<thead>
<tr>
<th>8.8 Anti-virus software is in operation and updated regularly.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Inspection</strong> Confirmed via examination of the network configurations that up-to-date anti-virus software is in operation.*</td>
</tr>
<tr>
<td><strong>No exceptions to the company’s procedures were noted.</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>8.9 Firewalls are in place to protect the networks from malicious attack.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Inspection</strong> Confirmed that firewalls were in operation over the network.*</td>
</tr>
<tr>
<td><strong>No exceptions to the company’s procedures were noted.</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>8.10 IT security reviews are carried out by independent external consultants on a regular basis. Recommended action is undertaken where appropriate.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Inspection</strong> Confirmed via inspection of the consultant report, that an IT security review had taken place during the year and appropriate follow up action had taken place.**</td>
</tr>
<tr>
<td><strong>No exceptions to the company’s procedures were noted.</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>8.11 Filters are in place to manage email spam and viruses.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Inspection</strong> Confirmed via inspection of the network configuration that filters for email spam and viruses were in operation.*</td>
</tr>
<tr>
<td><strong>No exceptions to the company’s procedures were noted.</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>8.12 Email traffic of material size / containing specific criteria is blocked using filtering software. Group IT will release the email once confirmed as safe.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Inspection</strong> Confirmed via inspection of the network configuration, that emails of material size or which contain specific criteria are blocked using filtering software.**</td>
</tr>
<tr>
<td><strong>Enquiry</strong> Confirmed via enquiry with Group IT that blocked emails are fully reviewed in their content and attachments before being released.**</td>
</tr>
<tr>
<td><strong>No exceptions to the company’s procedures were noted.</strong></td>
</tr>
</tbody>
</table>

---

Appropriate measures are implemented to counter the threat from malicious electronic attack (for example firewalls and anti-virus software).

RPMM incorporates a number of IT security practices to ensure maximum environment stability and security with minimal downtime from potential security threats.

Our security measures are embedded right from employee appointment, whereby the new employee must attest to reading and understanding our Computer User Handbook and sign a confidentiality agreement upon joining the company.

Our Group IT team has policies in place for continual updating of operating systems with industry standard security patches and a 24-hour intrusion detection monitoring system is in place. We regularly appoint consultants to carry out independent IT security reviews; any findings arising from the review will be considered and where necessary, implemented by the Group IT team. Filtering tools and anti-virus software add further resilience to the threat of malicious attacks.

---

* Underlying test performed by the Reporting Accountants

** Underlying test performed by RPMI Business Assurance team, subsequently reviewed by the Reporting Accountants.
The physical IT equipment is maintained in a controlled environment.

Our critical IT infrastructure is maintained in a secure and controlled environment with access limited to key staff. We have separate uninterrupted power supplies (UPS) to this IT equipment which would enable a clean shutdown of operations in the event that the main power supply fails.

The virtual server environment is also replicated to an offsite data centre which guarantees hardware availability; this also benefits from redundant capacity components; dual powered equipment; and is ISO 27001 accredited.

Back-up tapes are prepared on a daily basis and retained in an offsite commercial data archiving facility via a secure collection process.

We maintain an asset register which is updated to reflect changes in IT inventory and to allocate ownership of our assets. Authorisation from senior management is required for staff using IT equipment, such as laptops and mobile phones. All equipment loaned is logged and our employee leaver process ensures that such equipment is returned.

All company laptops and portable devices including mobile phones have enforced password requirements.

<table>
<thead>
<tr>
<th>Detailed controls</th>
<th>Relevant exceptions ‘if any’</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.13 IT infrastructure rooms are protected against fire, power failure and unauthorised access.</td>
<td>Inspection Confirmed that environmental controls were in operation in the server rooms.* No exceptions to the company’s procedures were noted.</td>
</tr>
<tr>
<td>8.14 The offsite data centre which is ISO 27001 accredited has the following security measures in place: 24/7 security monitoring, CCTV, electronic key access and security alarm.</td>
<td>Inspection Confirmed via inspection of the accreditation certificate that the data centre is ISO 27001 Information Security accredited.* Enquiry Confirmed via enquiries made with the data centre representatives that no changes to the IT security environment had taken place.* No exceptions to the company’s procedures were noted.</td>
</tr>
<tr>
<td>8.15 An IT asset register is maintained and updated for any purchases and disposals of equipment.</td>
<td>Inspection Confirmed that an asset register for IT equipment was maintained and that a sample of assets had been correctly recorded.* No exceptions to the company’s procedures were noted.</td>
</tr>
<tr>
<td>8.16 Company assets allocated to individuals are recorded in a central HR system. When an employee leaves the company, a checklist is completed to ensure Group IT are instructed to secure the return of the asset.</td>
<td>Inspection Confirmed for a sample of leavers, that the leaver checklist had been completed and company assets returned.* No exceptions to the company’s procedures were noted.</td>
</tr>
<tr>
<td>8.17 Laptops are encrypted or password protected and portable devices have mandatory password requirements.</td>
<td>Inspection Confirmed for a sample of laptops and portable devices in use, that encryption and password requirements have been applied.** No exceptions to the company’s procedures were noted.</td>
</tr>
</tbody>
</table>

* Underlying test performed by the Reporting Accountants  
** Underlying test performed by RPMI Business Assurance team, subsequently reviewed by the Reporting Accountants.
9. Maintaining and developing systems hardware and software

Development and implementation of new systems, applications and software, and changes to existing systems, applications and software, are authorised, tested, approved and implemented.

RPMI adopts formal project management methodologies to facilitate changes and/or implement new systems. These methods ensure that appropriate authorisation, testing and approvals are granted in controlled test environments before being released into live production.

The development process includes rigorous unit and integration testing and where necessary, functionality and user acceptance testing is performed.

Tailored training for the end-user forms a key part of the development process for major system changes, ensuring that the functionality and system design is in line with users’ needs.

Where there is a significant development, post-implementation reviews will be carried out to consider issues such as performance, usability and reliability.

A formal change management process is followed when changes are made to systems and critical data. All changes must be authorised and there is segregation between those requesting and approving the change.

<table>
<thead>
<tr>
<th>Detailed controls</th>
<th>Relevant exceptions ‘if any’</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.1 Project management tools are used to implement system developments.</td>
<td>Inspection  Confirmed for a sample of system developments that project management tools had been used.* No exceptions to the company’s procedures were noted.</td>
</tr>
<tr>
<td>9.2 Systems changes are appropriately authorised prior to being made in a live environment.</td>
<td>Inspection  Confirmed for a sample of system changes, that the change had been authorised prior to going live.* No exceptions to the company’s procedures were noted.</td>
</tr>
<tr>
<td>9.3 There is a distinct segregation between the live and test environments.</td>
<td>Inspection  Confirmed for a sample of systems / applications, that independent live and test environments are in place.** No exceptions to the company’s procedures were noted.</td>
</tr>
<tr>
<td>9.4 Testing is carried out in advance of systems being integrated into the production environment.</td>
<td>Inspection  Confirmed for a sample of system developments deployed into the production environment that appropriate testing had been undertaken and issues arising appropriately resolved.** No exceptions to the company’s procedures were noted.</td>
</tr>
</tbody>
</table>

* Underlying test performed by the Reporting Accountants
** Underlying test performed by RPMI Business Assurance team, subsequently reviewed by the Reporting Accountants.
Data migration or modification is authorised, tested and, once performed, reconciled back to the source data.

A standard approach is adopted for the validation and loading process for data migrations from third party sources. All data is subject to thorough data cleansing with validation testing carried out as appropriate. Accuracy and completeness reviews are carried out as part of the data reconciliation process to ensure the migration has been successful.

Parallel payroll running is carried out for a number of pay cycles to ensure information is consistent and accurate before administration is undertaken in the live system.

All data migrations require sign-off before the data is transferred into the live environment.
10. Recovering from processing interruptions

Data and systems are backed up regularly, retained offsite and regularly tested for recoverability.

Our systems and data are replicated at our remote storage area network or back-up tapes prepared daily and retained in an offsite commercial data archiving facility via a secure collection process.

We routinely test all servers for recoverability and maintain a log documenting the results. Where issues have arisen, action is taken and this is noted on the log.

<table>
<thead>
<tr>
<th>Detailed controls</th>
<th>Relevant exceptions ‘if any’</th>
</tr>
</thead>
</table>
| 10.1 Servers are replicated to an offsite datacentre or are backed up to tapes daily and taken to an offsite data storage facility. Daily reports are received confirming the results of the replication. | Inspection
Confirmed through review of daily confirmation reports, that servers had been successfully replicated to an offsite datacentre. Through review of record logs it was confirmed that for those servers not using the replication environment, regular back-ups were made to tape and retained in an offsite archiving facility.**
No exceptions to the company’s procedures were noted. |
| 10.2 Recoverability testing is undertaken on a regular basis with exceptions investigated and corrected. | Inspection
Reviewed the results of the recoverability testing and where exceptions were highlighted, obtained evidence to support an appropriate resolution had taken place.**
No exceptions to the company’s procedures were noted. |

IT hardware and software issues are monitored and resolved in a timely manner.

We have a dedicated Service Desk team within Group IT responsible for responding to user requests and issues.

The team uses an electronic Service Desk system to log incidents reported and assign a priority to enable resources to be directed more effectively. Each incident has a unique reference and once logged the user will receive automated emails informing them of progress. SLAs are in place for response and resolution times and are regularly monitored.

RPMI uses external hardware providers and the relationship with these providers is monitored regularly by the Group IT team to ensure the service provision is adequate.

* Underlying test performed by the Reporting Accountants
** Underlying test performed by RPMI Business Assurance team, subsequently reviewed by the Reporting Accountants.
Business and information systems recovery plans are documented, approved, tested and maintained.

We are ISO 22301 Business Continuity Management accredited. This means we provide a strategic and operational framework to improve resilience and restore critical functions following an incident.

As part of our Business Continuity arrangements, the following resources are in place:

- Business Continuity Plans for each business stream;
- continuous testing regimes to ensure Plans remain current and effective;
- Business Impact Analysis for critical functions including recovery time objectives and maximum tolerable period of disruption;
- alternative offsite recovery facilities for recovery of IT systems, provision of workplace recovery and helpline and telephony services; and
- regular training and awareness sessions for employees.

In the event of a major incident, business critical computer processing and services will be transferred to one of the designated remote recovery sites.

The IT Governance Manager is the RPMI Business Continuity Manager and is responsible for overseeing all plans and strategies. A Business Continuity Steering Group, comprising members from all areas of the business, meets regularly to discuss the overall Business Continuity Plan, review and update business-area specific plans, continually develop risk management and remain compliant with industry best practice.

Senior Executives are presented with the Business Continuity Plan annually for review and comment.
### 10.5 The Business Continuity Plans are ISO 22301 accredited, identify business critical areas and are subject to regular review and testing.

**Detailed controls**
- Underlying test performed by the Reporting Accountants

**Relevant exceptions ‘if any’**
- Inspection
  - Confirmed that business critical areas are identified in the Business Continuity Plan and that the Plan is subject to regular review and testing.*
  - No exceptions to the company’s procedures were noted.

### 10.6 The Business Continuity Steering Group, comprising cross-departmental representatives, meets regularly to ensure that the Plan remains relevant and is updated and distributed as necessary.

**Detailed controls**
- Underlying test performed by RPMI Business Assurance team, subsequently reviewed by the Reporting Accountants.

**Relevant exceptions ‘if any’**
- Inspection
  - Confirmed via inspection of the Business Continuity Steering Group’s terms of reference and meeting minutes that meetings are regularly held. Reviewed the plan currently available on the company intranet and confirmed this was the current version.*
  - No exceptions to the company’s procedures were noted.

### 10.7 A contractual agreement is in place with an alternative service provider in the event that business offices are unavailable.

**Detailed controls**
- Underlying test performed by the Reporting Accountants

**Relevant exceptions ‘if any’**
- Inspection
  - Confirmed via inspection of the contract with the workspace facility provider, that it will be available for key staff in the event it is necessary to relocate operations.*
  - No exceptions to the company’s procedures were noted.

### 11. Monitoring compliance

**Outsourced activities are properly managed and monitored.**

The majority of IT services are provided by our in-house Group IT team. Where there are outsourced services, periodic reporting from the outsourced provider is received. The reporting includes analysis of the service provision and performance responses for the period. These reports are reviewed by the IT Governance Manager and discussed with the provider.

**Detailed controls**
- Underlying test performed by RPMI Business Assurance team, subsequently reviewed by the Reporting Accountants.

**Relevant exceptions ‘if any’**
- Inspection
  - Confirmed via inspection that contracts are in place with critical hardware and software providers.*
  - Enquiry
    - Confirmed through discussion with the IT Governance Manager and Senior Client Services Manager that service providers are subject to regular review and monitoring.*
  - No exceptions to the company’s procedures were noted.
03 Report by the Reporting Accountants
Reporting accountants’ assurance report on internal controls of service organisation to the directors of RPMI Limited

Use of report
This report is made solely for the use of the directors, as a body, of RPMI Limited (RPMI), and solely for the purpose of reporting on the internal controls of RPMI in accordance with the terms of our engagement letter dated 1 July 2014 and found on pages 61-70.

Our work has been undertaken so that we might report to the directors 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, to the Railways Pension Trustee Company Limited (RPTCL) and clients (using RPMI’s pensions administration services) (clients), and to the auditors of RPTCL and such clients to enable RPTCL, clients and their auditors to verify that a report by reporting accountants has been commissioned by the directors of RPMI and issued in connection with the internal controls of RPMI and without assuming or accepting any responsibility or liability to clients or their auditors on our part.

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

Scope
We have been engaged to report on RPMI’s description of its pensions administration services throughout the year ended 31 December 2014 (the description), and on the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description.

Service organisation’s responsibilities
RPMI is responsible for: preparing the description and the accompanying assertion set out on page 6, including the completeness, accuracy, and method of presentation of the description and the assertion; providing the services covered by the description; specifying the criteria including the control objectives and stating them in the description; identifying the risks that threaten the achievement of the control objectives; and designing, implementing and effectively operating controls to achieve the related control objectives stated in the description.

The control objectives stated in the description include the internal control objectives developed for service organisations as set out in the ICAEW Technical Release AAF 01/06.

Reporting accountants’ responsibilities
Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in that description. We conducted our engagement in accordance with International Standard on Assurance Engagements 3000 and 3402, and ICAEW Technical Release AAF 01/06. That standard and guidance require that we comply with ethical requirements and plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description, throughout the year ended 31 December 2014.

Our work involved performing procedures to obtain evidence about the presentation of the description of the pensions administration services and the design and operating effectiveness of those controls. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related control objectives stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the description and the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organisation and described on pages 16-17.
Inherent limitations
RPМI’s description is prepared to meet the common needs of a broad range of customers and their auditors and may
not, therefore, include every aspect of the service organisation activities or system that each individual customer may
consider important in its own particular environment. Also, because of their nature, controls at a service organisation may
not prevent or detect and correct all errors or omissions in processing or reporting transactions.

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

Opinion
In our opinion, in all material respects, based on the criteria including specified control objectives described in the
directors’ assertion on page 6:

a) the description on pages 16-56 fairly presents the pensions administration services that were designed and
implemented throughout the year ended 31 December 2014;
b) the controls related to the control objectives stated in the description on pages 16-56 were suitably designed to
provide reasonable assurance that the specified control objectives would be achieved if the described controls
operated effectively throughout the year ended 31 December 2014;
c) the controls that were tested were operating with sufficient effectiveness to provide reasonable assurance that the
related control objectives stated in the description were achieved throughout the year ended 31 December 2014.

Description of tests of controls
The specific controls tested and the nature, timing and results of those tests are detailed on pages 16-56.
Engagement Letter

1 July 2014

Private and confidential

The Board of Directors
RPMI Limited
Stooperdale Offices
Brinkburn Road
Darlington
County Durham
DL3 6EH

Dear Sirs

Engagement letter – ISAE 3402 / AAF 01/06 Type II Reporting Accountants’ Assurance Report

Thank you for appointing Assure (UK) Limited as Reporting Accountants. This engagement letter and our Terms of Business set out in the Schedule to this engagement letter (together, “Agreement”) set out the terms on which Assure (UK) Limited (“Assure UK”, “we”, “our” or “us”), are instructed. We should be grateful if you would confirm in writing your agreement to these terms by signing and returning the enclosed copy of this letter.

Our Instructions

We are instructed by RPMI Limited (“Service Organisation”, “you” or “your”) to provide professional services to report to you on your internal controls with respect to the pension administration services provided by RPMI Limited in Darlington and EPAL Limited (trading as “RPMI EPAL”) in Coventry (“Assurance Report”).

The Assurance Report will review the control procedures in place in the Service Organisation and the suitability and effectiveness of these control procedures during the year ending 31 December 2014 in accordance with the International Standard on Assurance Engagements 3402 “Assurance reports on controls at a Service Organisation” issued by the International Auditing and Assurance Standards Board (“ISAE 3402”), and Technical Release AAF 01/06 “Assurance reports on internal controls of service organisations made available to third parties” issued by the Institute of Chartered Accountants in England and Wales (“AAF 01/06”).

Further details regarding the Assurance Report can be found in the attached Schedule.

Subject to the Permitted Disclosures set out in this Agreement (see clause 5 of our Terms of Business), the Assurance Report will be made solely for the benefit of the Service Organisation and its directors or partners (“Directors”) and solely for the purpose of reporting on the Service Organisation’s controls, in accordance with this Agreement (“Purpose”).

Special arrangement

We understand that you wish to make a copy of our Report available on your website. We give consent on the basis that you agree to the wording in appendix 3 to be included on your website and on the basis that our report can only be viewed to those website visitors who confirm they have read and agree the wording set out in appendix 3.
Terms of Business

Our Terms of Business are attached in the Schedule. Any work already performed in connection with this engagement before the date of this letter will also be governed by this Agreement.

We draw your attention to clause 7 of our attached Terms of Business which amongst other things limits our total liability to you under this Agreement to £1,000,000 and clause 18.3 which shortens the period within which any claim may be commenced.

This Agreement may only be varied or modified in accordance with clause 9 of the Terms of Business and we draw your attention to clause 8 which sets out the provisions for terminating this Agreement.

If you have previously instructed Ash Shaw LLP and provided documents relating to those instructions to Ash Shaw LLP, all such documents shall be passed to us in order for us to undertake the Assurance Report. You consent that such documents may be passed to us by Ash Shaw LLP for this purpose.

Fees

Our fees will be agreed separately in writing prior to the commencement of our work and the basis of our fees is set out in the attached terms of business at clause 14.

Agreement of Terms

Please confirm you accept this Agreement by signing the enclosed copy letter and returning it to us but, if you do not do so, your continuing to instruct us will signify your acceptance of this Agreement.

If you have any questions, please contact Andrew Riley on 020 7462 8410.

We are very much looking forward to working with you.

Yours faithfully

Assure (UK) Limited

Copy letter to be returned to Assure (UK) Limited

The terms and conditions contained in this letter and attached terms of business are agreed and accepted.

Signature of authorised person on behalf of RPMI Limited

Print name: Chris Hitchen

Position: Chief Executive

Date: 3/10/14
Schedule: Terms of Business

1. INTRODUCTION

1.1. These terms apply to the services we are instructed to provide under this Agreement. If anything in these terms of business is inconsistent with the engagement letter, the terms of business shall take precedence unless the engagement letter specifically amends them.

1.2. This Agreement will start on the earlier of the date of the attached engagement letter or the commencement of the services described in this Agreement.

2. THE ASSURANCE REPORT

2.1. In providing the Assurance Report we shall review the Directors’ written report on the internal controls at specified business units for the relevant period in accordance with ISAE 3402 and AAF 01/06 (“Directors’ Control Report”), enquiries of the management at the specified business units, review the relevant documentation prepared by the Service Organisation and observe and test specific control procedures as identified in the Directors’ Control Report. The tests we perform shall be itemised in an appendix to our Assurance Report.

2.2. To complete our Assurance Report we may seek written representations from the Directors and others about the internal controls identified in the Directors’ Control Report. We may request the Directors to provide written confirmation of oral representations received as part of these enquiries.

2.3. We may seek written representations from the Directors in relation to matters on which independent corroboration is not available. We shall seek confirmation from the Directors that all matters of which we should be aware have been brought to our attention.

2.4. The results of our review and the written representations will comprise the evidential matter on which we shall reach our independent conclusions of the description, design and suitability of the internal controls identified to us in relation to the provisions of pensions administration services as set out in the Assurance Report.

2.5. If for any reason we are unable to complete our review we may decline to issue the Assurance Report.

2.6. Where the Assurance Report is made available to you in electronic format as well as hard copy format, and multiple copies and versions of the Assurance Report exist in different media, the signed hard copy should be regarded as definitive.

3. YOUR RESPONSIBILITIES

3.1. The Directors are responsible for the design, implementation and operation of control procedures that provide an adequate level of control over the pensions administration services they provide, including, but not limited to:

- acceptance of responsibility for internal controls;
- evaluation of the effectiveness of the Service Organisation’s control procedures using suitable criteria;
- supporting their evaluation with sufficient evidence, including documentation; and
- providing in the Directors’ Control Report an assertion as to the effectiveness of the Service Organisation’s internal controls for the relevant period.

3.2. In drafting the Directors’ Control Report, the Directors shall have regard to, as a minimum, the criteria specified within ISAE 3402 and control objectives specified in AAF 01/06 but they may add to these criteria to the extent reasonably necessary.
3.3. The Directors shall make available to us, on a timely basis, all information which we consider reasonably necessary for performing our review and testing and to enable us to contact Service Organisation personnel to whom we may direct enquiries. The Directors are responsible for ensuring that the information provided to us, whether by the Directors or any other person working for or on behalf of the Service Organisation, is accurate and complete. We will not verify any information given to us relating to this engagement.

3.4. Subject to clause 7, you hereby release and shall indemnify us from all liabilities, costs, claims and expenses (including without limitation, reasonable legal fees) on a full indemnity basis relating to our Assurance Report which relates to any misrepresentations or information which is withheld or concealed from us except where liability or costs arise from our knowing disregard.

4. INHERENT LIMITATIONS OF CONTROL PROCEDURES

4.1. You acknowledge that controls designed to address specific control objectives are subject to inherent limitations and accordingly, errors or irregularities may occur and not be detected. Such controls cannot guarantee protection against (amongst other things) fraudulent collusion especially on the part of those holding positions of authority or trust. If any such matters come to our attention we may communicate these matters to the Directors or other personnel as appropriate.

4.2. The Directors’ Control Report and our Assurance Report will be based on historical information and the projection of any information or conclusions in these reports to any future periods would be inappropriate. In addition this Assurance Report is prepared in respect of the relevant period to which it relates. As such, any reliance upon it should be tempered accordingly.

4.3. The effectiveness of specific controls at the Service Organisation is dependent on how these controls interact with the controls and other factors present at individual client organisations. We will not review the effectiveness of controls at individual client organisations.

5. YOUR USE OF THE ASSURANCE REPORT

5.1. Subject to clause 5.3, the Assurance Report will be issued on the understanding that you may not recite, refer to or disclose the whole document or part of it, whether in electronic format or otherwise, to any party without the prior written permission of one of our Directors. Permission from any other person shall not constitute valid consent.

5.2. Subject to clause 5.3, the Assurance Report will be issued solely for the purpose of reporting on the Service Organisation’s controls, in accordance with this Agreement.

5.3. We permit the disclosure of the Assurance Report in the following circumstances (“Permitted Disclosures”) provided there is no change to the wording, form, content, context or presentation of the Assurance Report:

5.3.1. As a complete document, in electronic format or otherwise, to existing clients using the Service Organisation’s pensions administration services, and to the auditors of the Service Organisation and such existing clients (“Permitted Recipients”) pursuant to 5.4 and 5.5 for the sole purpose of verifying that the Assurance Report has been commissioned. In permitting this disclosure we do not accept responsibility or liability to the Service Organisation’s clients or their respective auditors.

5.3.2. As a complete document, in electronic format or otherwise, to the Service Organisation’s prospective clients only where this disclosure is made with the attached Disclaimer Letter (appendix 2) published in the appendix to the Assurance Report and that this Disclaimer Letter is brought to the attention of the prospective client by the inclusion of a prominent disclaimer at the front of the Assurance Report. In permitting this disclosure we do not accept any responsibility or liability to the Service Organisation’s prospective clients.
5.4. We will allow the Permitted Disclosures in 5.3.1 provided that the Permitted Recipients first accept in writing, in the form of the attached Acknowledgment Letter at appendix 1, the relevant terms of this Agreement as if the Client had signed the Agreement when originally issued, including the provisions limiting our liability in respect of the Assurance Report, usage restrictions, limitations and exclusions in return for the opportunity to verify that the Assurance Report has been commissioned. Each Client who signs the acknowledgment letter shall be a party to this Agreement unless we, in our absolute discretion, decide otherwise.

5.5. In the alternative to clause 5.4, we will allow the Permitted Disclosures in 5.3.1 without the Permitted Recipients having first accepted in writing the terms of this Agreement in the form of the acknowledgement letter at appendix 1 provided that you hereby indemnify and shall keep indemnified Assure UK, its directors and employees against all losses, damages, and expenses (including, without limitation, reasonable legal expenses) suffered or incurred by any of the same as a result of any claim or action brought by the Permitted Recipients following the Permitted Disclosure at 5.3.1.

5.6. We may request amendments to the electronic version of the Assurance Report if we are not satisfied with the proposed wording or its presentation or the manner in which it is published. If requested you shall promptly provide us with full cooperation and assistance to make such amendments and shall withdraw any previous or existing versions of the Assurance Report from circulation and shall promptly ensure that the same are no longer available for download or other review or access.

5.7. Where the Directors or the Service Organisation prepare marketing literature referring either to us or the Assurance Report you will first obtain our prior written consent before publishing such literature.

5.8. Subject to clause 7, we accept no responsibility for any changes that may occur to our Assurance Report made after a permitted disclosure or a disclosure in breach of this Agreement. If we do become aware of any amendments we will notify the Directors that the report no longer corresponds to the Assurance Report issued by us.

6. ACCESS TO WORKING PAPERS

6.1. Our working papers and other internal documentation created for the purpose of carrying out our engagement under this Agreement belong solely to Assure UK and will not be provided to you.

6.2. We may be required to give access to our working papers for regulatory purposes or because of other statutory obligations. Unless we are prevented from doing so by legislation, regulation, court order or other professional or legal requirement, we will notify you prior to giving access to our working papers.

7. LIMITATION OF LIABILITY

7.1. The following provisions set out our entire financial liability to the Service Organisation and the Directors during the course of our engagement under the Agreement or otherwise (including, without limitation, any liability for the acts or omissions of our employees, agents and sub-contractors) in respect of (a) any breach of the Agreement howsoever arising; and (b) any representation, misrepresentation (whether innocent or negligent), statement or tortious act or omission (including, without limitation, negligence) arising out of or in connection with the Agreement.

7.2. All warranties, representations, conditions and other terms implied by statute or common law are excluded from the Agreement to the fullest extent permitted by law.

7.3. Nothing in this Agreement excludes or limits our liability for (a) death or personal injury caused by our negligence; or (b) fraud or fraudulent misrepresentation or (c) anything else that may not be excluded or limited under applicable law.
7.4. Subject to clause 7.2 and clause 7.3:

7.4.1. We shall not in any circumstances be liable, whether in tort (including, without limitation, for negligence or breach of statutory duty howsoever arising), contract, misrepresentation (whether innocent or negligent) or otherwise for any special, indirect, consequential or pure economic loss, costs, damages, charges or expenses.

7.4.2. Our total liability in contract, tort (including, without limitation, negligence and breach of statutory duty howsoever arising), misrepresentation (whether innocent or negligent), restitution or otherwise, arising in connection with the performance or contemplated performance of the Agreement or otherwise shall be limited to £1,000,000.

7.4.3. We shall not be liable for any losses which are due to the provision of false, misleading or incomplete information or documentation or due to the acts or omissions of any person other than us, except where, on the basis of the enquiries normally undertaken by us within the scope set out in this Agreement, it would have been reasonable for us to discover such defects.

7.5. Where we agree in writing to accept liability to more than one party, the limit on our liability in clause 7.4.2 will be shared between the parties and it will be for those parties to decide how to share it.

7.6. Where any loss is suffered by you for which Assure UK and any other person are jointly and severally liable, the loss recoverable by you from us shall be reduced so as to be in proportion to our relative contribution to the overall fault of Assure UK, the Service Organisation and any other person in respect of the loss in question. In determining the extent of the contribution to the overall fault of any other person no account shall be taken of any limit or exclusion placed on the amount that person will pay or any shortfall in recovery from that person (for whatever reason).

7.7. To the fullest extent permissible by law, you hereby indemnify and shall keep indemnified Assure UK, its directors and employees against all losses, damages, and expenses (including reasonable legal expenses) suffered or incurred by any of the same as a result of any breach of this Agreement by the Service Organisation, its Directors, employees, contractors or agents including without limitation clause 5 relating to your use of our Assurance Report.

7.8. To the fullest extent permissible by law, you agree to bring any claim (including negligence) in connection with this Agreement against Assure UK and not against any individual employed by us.

7.9. You shall ensure that none of the Service Organisation's group companies, including any subsidiary, associated or holding company (unless a party to this Agreement), while they are a group company or at any time after, bring a claim against Assure UK (or its directors or employees) or our subcontractors in respect of any liability relating to the services provided under this Agreement.

8. TERMINATION

8.1. Our appointment under this Agreement may be terminated immediately by you or us by giving notice in writing where (a) there is a material breach of the Agreement that is not rectified within 14 days of the breach (b) the performance of the Agreement may breach a legal or regulatory requirement (c) you or we appear likely to be unable to pay debts or become insolvent.

8.2. Our Appointment under this Agreement may be terminated by you or us by giving 30 days’ notice in writing.
9. ENTIRE AGREEMENT

9.1. This Agreement constitutes the sole and entire understanding of the parties in relation to the subject matter of this Agreement and supersedes all previous agreements, representations and arrangements between the parties (either oral or written) with regard to the subject matter of this Agreement other than where such agreements have been expressly included by reference. The parties confirm that they have not entered into this Agreement on the basis of any representations that are not expressly incorporated in this Agreement. Each party irrevocably and unconditionally waives any rights it may have to claim damages and/or to rescind this Agreement for any misrepresentation in relation to the subject matter of this Agreement whether or not contained in this Agreement or for breach of warranty not contained in this Agreement unless such misrepresentation or warranty was made fraudulently. This Agreement may only be amended or supplemented in writing and signed by an authorised representative of both parties.

9.2. Subject to clause 7.3, neither party is liable to any other party (in negligence or otherwise) for a representation relating to this Agreement whether in this Agreement or otherwise or for a breach of warranty not contained within this Agreement.

9.3. This Agreement may only be amended or supplemented in writing and signed by an authorised representative of both parties.

9.4. Any provisions of this Agreement which by their nature extend beyond the expiry, completion or termination of this Agreement shall survive such expiration, completion or termination.

10. CONTRACTING PARTIES AND ASSIGNMENT

10.1. We may provide certain services under this Agreement by using personnel provided to Assure UK through subcontracting agreements. We remain solely responsible to you in connection with the services provided under this Agreement and subject to clause 7.3 you agree not to bring any claim (whether in contract, tort, breach of statutory duty or otherwise and including but not limited to, a claim for negligence) against our subcontractors in connection to the services provided under this Agreement.

10.2. This Agreement does not make either of us an agent or legal representative of the other, nor does it create a partnership or joint venture.

10.3. Where you consist of more than one party, an act or omission of one party will be regarded as an act or omission of all.

10.4. You may not assign or otherwise transfer the benefit of this Agreement without our prior written consent.

10.5. Except as provided at clauses 5.4, 7.5 and 10.1, no person who is not a party to the Agreement shall have any rights under the Contracts (Rights of Third Parties) Act 1999 to enforce any of its terms. This Agreement can be varied without any third party’s consent.

11. GENERAL UNDERTAKINGS AND CONFIDENTIALITY

11.1. We undertake to carry out the engagement under this Agreement with reasonable care and skill.
11.2. We will not accept any responsibility for any reliance that may be placed by any third parties on either our assurance reports which are provided by us to you or on any other reports or work products which are provided by us to you for your sole use, unless our prior written consent is obtained for the provision of particular reports or work products to specified third parties and is given in writing prior to the provision of any reports or work products. Such consent will be granted only on the basis that our reports or work products are not prepared with the interests of anyone other than you in mind and that we accept no duty or responsibility to any other party as concerns the reports or work products and that each specified third party acknowledges and accepts this (or such other terms as we may in our discretion agree with them) in writing directly with us.

11.3. We will not disclose any confidential information concerning your business to third parties (except to our employees, partners, agents and other professional advisers whom we may consult in relation to our work and save to the extent that the information is in the public domain) without your prior written consent unless otherwise required by law, a court of competent jurisdiction, The Pensions Regulator, HM Inland Revenue or other government or regulatory authority. Subject to the foregoing, we may disclose your confidential information to our affiliates and subcontractors including those engaged in support of our office administration.

11.4. All information and advice, written or oral, of whatever nature, made available by us to you is for your sole use and shall not, subject to the provisions of clause 5, be disclosed or made available to any third party (save to the extent that the same is in the public domain otherwise than by breach of this clause) without our prior written consent unless otherwise required by law, a court of competent jurisdiction, The Pensions Regulator, HM Inland Revenue or other government or regulatory authority.

11.5. The working papers prepared in conjunction with our audit and other services are the property of our firm, constitute confidential information and will be retained by us in accordance with our firm’s policies and procedures.

11.6. Nothing in this document precludes us or any of our directors or employees from taking such steps as are necessary to comply with professional or ethical rules of any relevant professional body of which our director or employee is, at the time, a member.

11.7. We may outsource certain services including IT support, our “front office” and “back office” functions, photocopying and word processing to carefully selected service providers, with whom we have agreed confidentiality provisions and undertakings; some of these outsourced service providers may transfer your personal data outside the European Economic Area (EEA). By accepting the terms of this agreement, you consent to these outsourcings and the transfer of your personal data outside the EEA.

11.8. We may wish to refer to you and the services provided to you under this Agreement as part of our marketing material. You hereby agree that we may do so provided we do not disclose your confidential information.

12. INTELLECTUAL PROPERTY

12.1. We will own the intellectual property rights in the Assurance Report and any other deliverables or materials created or provided under this Agreement, and subject to clause 5, we hereby grant the Service Organisation a non-exclusive, non-transferable licence to use the Assurance Report for the Purpose.

13. ELECTRONIC COMMUNICATIONS

13.1. We may correspond with you electronically (unless you expressly request otherwise on specific matters) and receive such communications from you. We may also, with your agreement, use electronic means of communication to send and receive information requests and confirmations to and from designated third parties in connection with the Assurance Report.
13.2. You and we understand and acknowledge that the electronic transmission of information by e-mail on the Internet or otherwise has inherent risks and that such communications may become lost, delayed, intercepted, corrupted or be otherwise altered, rendered incomplete or fail to be delivered. We shall use commercially reasonable procedures to ensure that such electronic communications are free from viruses and any other material which may cause inconvenience or harm to any other computer system and you undertake to do likewise with any electronic communications you send to us. As the electronic transmission of information cannot be guaranteed to be secure or error-free and its confidentiality may be vulnerable to access by unauthorised third parties, we shall not have any responsibility or liability to you on any basis other than our bad faith or willful default in respect of any electronic communication of information by us to you or your other advisers.

14. FEES AND EXPENSES

14.1. Unless we have agreed otherwise, we will present invoices on account as our work progresses, which will be due for payment on presentation of an invoice. We may charge interest at 3% above Barclays Bank PLC’s base rate per annum on overdue amounts.

14.2. Cash will not be accepted in payment for services rendered. All fees should be paid by cheque or, preferably, by bank transfer.

14.3. Travelling, subsistence, accommodation, report production, any special telecommunications or computing charges and any other expenses properly incurred while engaged on your business, whether at your premises or elsewhere, are charged at cost.

14.4. You will also pay any taxes, including VAT, that are due in relation to our goods and services under this Agreement. You will pay the full amount of any invoice regardless of any deduction that you are required to make.

14.5. Where fees are charged on an hourly basis, these charge out rates may be reviewed from time to time and may be increased. We shall notify you of any increase. We reserve the right to vary the rates to reflect discretionary factors such as unusual urgency, complexity, the responsibility involved, transaction value and/or out of hours working.

14.6. If we terminate this Agreement in accordance with clause 8 we shall be entitled to the fees incurred until the date the engagement is terminated notwithstanding that the work we have undertaken may not be complete at the termination date.

15. DATA PROTECTION

15.1. For the purposes of the Data Protection Act 1998, you are the data controller and we act as the data processor of any Personal Data. In this Agreement, Personal Data shall have the meaning set out in section 1(1) of the Data Protection Act 1998 and relates only to personal data, or any part of such personal data, of which you are the data controller and in relation to which we are providing services under this Agreement.

15.2. We shall process the Personal Data only to the extent necessary to fulfill the services under this Agreement and/or in accordance with your instructions from time to time and shall not process the Personal Data for any other purpose. For the purposes of this clause processing and process and data subject shall have the meaning set out in section 1(1) of the Data Protection Act 1998.

15.3. If we receive any complaint, notice or communication which relates directly or indirectly to the processing of the Personal Data or to either party’s compliance with the Data Protection Act 1998 and the data protection principles set out therein, we shall immediately notify you and shall provide you with full co-operation and assistance in relation to any such complaint, notice or communication.
15.4. We will maintain reasonable administrative, physical and technical safeguards against the unauthorised or unlawful processing of personal data and against the accidental loss or destruction of, or damage to, personal data.

16. QUALITY OF SERVICE

16.1. Our objective is to seek to provide you with the highest quality of service to meet your needs. If at any time you would like to discuss with us how our service to you could be improved or if you are in any way dissatisfied with the service you are receiving, please raise the matter with the director responsible for providing the services under this Agreement to you. If you would prefer to discuss the matter with someone other than that director, or you wish to make a complaint please call or write to Lorraine Hawkins, Assure UK’s nominated Complaints Officer.

16.2. We undertake to look into any complaint carefully and promptly and to do all we can to resolve the position to your satisfaction. If by this process we are unable to meet your concerns, you may then take up the matter with the Institute of Chartered Accountants in England and Wales. To contact the ICAEW, write to the Professional Standards Office, Metropolitan House, 321 Avebury Boulevard, Milton Keynes MK9 2FZ.

17. INVALIDITY

17.1. If any provision of this Agreement is held to be illegal, invalid or unenforceable, in whole or in part, under any enactment or rule of law, such provision or part shall, to that extent, be deemed not to form part of this Agreement but the legality and enforceability of the remainder of this Agreement shall not be affected.

18. APPLICABLE LAW

18.1. This Agreement shall be governed by, and construed in accordance with, English law. The Courts of England shall have exclusive jurisdiction in relation to any claim, dispute or difference concerning this Agreement and any matter arising from it. Each party irrevocably waives any right it may have to object to an 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.

18.2. If any dispute arises in connection with this Agreement, the parties will first use reasonable endeavours to resolve the dispute amicably between them. If the dispute is not resolved either party may refer (by mutual written agreement) the dispute to an agreed mediator of suitable independence and skill to adjudicate on the matter. The mediator shall be deemed to act as an expert and not as an arbitrator. To initiate the mediation a party must give notice in writing (ADR notice) to the other party to the dispute requesting a mediation. The mediation will start no later than thirty (30) days after the date of the ADR notice. No party may commence any court proceedings in relation to any dispute arising out of this Agreement until it has attempted to settle the dispute by mediation and either the mediation has terminated or the other party has failed to participate in the mediation, provided that the right to issue proceedings is not prejudiced by a delay.

18.3. Any claims, whether in contract, negligence or otherwise, must be formally commenced no later than two (2) years after the party bringing the claim becomes aware (or ought reasonably to have become aware) of the facts which give rise to the action and in any event no later than four (4) years after any alleged breach of contract, negligence or other cause of action. This expressly overrides any statutory provision which would otherwise apply.

18.4. No party shall be liable to the other if it fails to meet its obligations because of matters beyond its reasonable control.

18.5. You are reminded that, in addition to the identity checks, which we undertake for all new clients, the Proceeds of Crime Act 2002 and the Money Laundering Regulations 2007 (as amended from time to time) place additional legal requirements on us.
Dear Sirs

Release of the 2014 internal controls assurance report to prospective clients and third parties

The 2014 report on internal controls in accordance with ISAE 3402 and AAF 01/06 which relates to the pension administration services provided by RPMI Limited in Darlington and EPAL Limited in Coventry ("Service Organisation") for the year ended 31 December 2014 ("2014 Directors’ Control Report") has been prepared by the Directors of the Service Organisation principally for the purposes of providing information to organisations who were clients at 31 December 2014. You have asked us to agree to you providing to prospective clients, i.e. organisations that were not clients at 31 December 2014, a copy of the 2014 Directors’ Control Report which includes our assurance report on internal controls ("Assurance Report") dated 10 March 2015.

We confirm that we are agreeable to you so doing on the clear understanding that our Assurance Report was addressed to you and was prepared on your instructions as set out in our engagement letter dated 1 July 2014.

The Assurance Report was not prepared for the benefit of any prospective clients or other third parties and therefore items of possible interest to prospective clients or third parties may not have been specifically addressed.

To the fullest extent permissible by law, Assure (UK) Limited makes no warranty or representation that the information in the Assurance Report is appropriate for the interests or purposes of prospective clients, or as to the truth and accuracy of the contents, including without limitation, as to whether the information has changed in any way since the date of the Assurance Report.

Therefore the Assurance Report cannot in any way serve as a substitute for enquiries and procedures that prospective clients would (or should) undertake for the purpose of satisfying themselves regarding any matters relating to the Service Organisation’s administration procedures of for any matter arising in the Assurance Report.

Assure (UK) Limited, its directors, employees and agents neither owe nor accept any duty or responsibility to prospective clients or third parties whether in contract or in tort (including, without limitation, negligence and breach of statutory duty) or however so arising. Assure (UK) Limited shall not be liable, and prospective clients and third parties shall not bring any action, proceeding or claim in respect of any loss damage or expense of whatsoever nature which results from any use of prospective clients or third parties choose to make of the Assurance Report, or any reliance they may seek to place on it.

The 2014 Directors’ Control Report and our Assurance Report contained within it are not to be copied in whole or in part in any document and may not be distributed without our prior written permission.

To ensure that prospective clients have a clear understanding of the terms under which our Assurance Report is being provided to them, a copy of this letter should accompany our Assurance Report.

Yours faithfully

Assure (UK) Limited