INTERNAL CONTROL ASSURANCE REPORT

Pension Administration

RAILPEN

2025

CONTENTS

INTRODUCTION

Railpen delivers high-quality pensions and investment services to the Railways Pension Trustee Company Limited (RPTCL). The pensions administration service has been provided for over 48 years and we also offer communications and employer covenant services to schemes and employers.

We are based at two sites, in Darlington and London. We currently look after the pension needs of over 150 Rail clients and care for over 350,000 members of the railway pension schemes.

This Internal Control Assurance Report outlines the specific control activities that we have designed to support the business objectives of the pensions administration services provided to our Rail clients. It underpins the work Railpen has undertaken over many years and, together with the Service Auditor's Assurance Report, independently demonstrates the strength of our control environment which supports our organisation as we move forward into the future.

This is our 22nd 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 01/20).

In total, Railpen manages

2 locations

• London • Darlington

Over 150 clients

Over 350,000 Scheme members

REPORT BY THE DIRECTORS

This report relates to the pensions administration services provided by Railpen Limited (Railpen), at its offices in Darlington, throughout the year ended 31 December 2025.

As Directors of Railpen we are responsible for the identification of control objectives relating to the provision of pensions administration and related information technology services by Railpen and the design, implementation and operation of Railpen's control activities to provide reasonable assurance that the control objectives are achieved.

In carrying out those responsibilities we have regard not only to the interests of 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 and related technology services and their auditors, who have sufficient understanding to consider the description, along with other information including awareness of Railpen's control activities operated by clients themselves.

We have evaluated the fairness of the description and the design suitability of Railpen's control activities in accordance with the Technical Release AAF 01/20 ('AAF 01/20'), issued by the Institute of Chartered Accountants in England and Wales, and the control objectives for pensions administration and related technology services set out in the AAF 01/20 and the International Standard on Assurance Engagements 3402 (ISAE 3402), issued by the International Auditing and Assurance Standards Board.

Railpen uses an Information Technology service organisation (the 'subservice organisation') for its systems development, data hosting and backups. The description includes only the control objectives and related controls of Railpen and excludes the control objectives and the related controls of the subservice organisation. The description does not extend to the controls of the subservice organisation.

We confirm that:

A. The accompanying description fairly presents Railpen's pensions administration and related information technology services for clients governed by RPTCL, as set out in pages 15 to 76 throughout the period from 1 January 2025 to 31 December 2025. In addition to the control objectives specified in AAF 01/20, the criteria used in making this statement was that the accompanying description:

i. Presents how the services were designed and implemented, including: the types of services provided, and as appropriate, the nature of transactions processed; the procedures, both automated and manual by which client and customer transactions were initiated, recorded, and processed; the accounting records and related data that were maintained, reported and corrected as necessary; the means by which the systems captured and addressed significant events and conditions, other than client and customer transactions; the process used to prepare reports for clients; relevant control objectives and controls designed to achieve those objectives; controls that we assumed, in the design of the system, would be implemented by users, and which, if necessary, to achieve control objectives stated in the accompanying description, are identified in the description along with the specific control objectives that cannot be achieved by ourselves alone; and other aspects of our control environment, risk assessment process, monitoring and information and communication systems, that were relevant to our control activities.

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

iii. Does not omit or distort information relevant to the scope of the services being described, while acknowledging that the description is prepared to meet the common needs of a broad range of clients and their auditors and may not therefore include every aspect of the services that each individual client may consider important in its own particular environment.

B. The control activities related to the control objectives stated in the accompanying description, as set out in pages 15 to 76 were suitably designed and operated effectively throughout the period 1 January 2025 to 31 December 2025. The criteria used in making this statement were that:

i. The risks that threatened achievement of the control objective stated in the description were identified.

ii. The identified control activities would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved.

iii. The control activities were consistently applied as designed, including manual controls which were applied by individuals who have the appropriate competence and authority.

As part of Railpen's commitment to delivering high quality pension and investment services we continued to review our administration systems and processes during 2025. Following our initial notification to The Pensions Regulator, as outlined in previous years' reports, we continued to work with them as we strengthened our control environment. We have previously commented that the impact and scale of the issues had materially reduced upon analysis. This continued to be the case in 2025. The issues have all now been resolved and project closure agreed with The Pensions Regulator, who has thanked us for the open, transparent, and collaborative way in which we engaged with them during the project.

The issues identified did not have an impact on the control activities applied during the year or the accompanying description stated above. The investigations and resolution activity continued in 2025 and the Executive Management continued to prioritise remediation efforts during that period.

Signed on behalf of the Board of Directors

Andy Bord
Chief Executive

22 July 2026

Complementary User Entity Controls

Railpen's controls cover only a portion of the overall internal control environment of each client. It is not feasible for the control objectives relating to pension administration services to be achieved solely by Railpen. A client's internal controls also form part of the control environment and must be evaluated in conjunction with our control activities.

The following notes the internal control responsibilities which address the interface and communication between Railpen and each client. For clients to rely on the control activities reported on herein, each client must evaluate its own internal controls to determine if the following control activities are in place. Clients should:

- Review and approve the scheme benefits schedule provided by Railpen during the transition process.
- Review and approve calculation specifications where required.
- Ensure contributions to pension schemes are submitted on a timely and complete basis.
- Communicate on a timely basis any changes to member records or the creation of new member records.
- Ensure member data exchange is protected via encryption tools/password security.
- Communicate in a timely manner with appropriate supporting documentation changes to individuals who are able to approve expenses.
- Notify Railpen in writing of changes to scheme design.

CONTROLS ASSURANCE FRAMEWORK

Organisational structure

Railpen is wholly owned by the Railways Pension Trustee Company Limited, RPTCL (the Trustee Company), and operates from two sites, in Darlington and London.

Railpen

Railpen looks after all administration and trustee services for the Railways Pension Scheme (RPS), other railway schemes. It looks after the needs of over 350,000 pension scheme members across a variety of schemes. It is responsible for pensions administration services including collection of contributions, payment of pension benefits and communications with members. The Industry-Wide Defined Contribution (IWDC) section of the RPS, is authorised as a Master Trust by The Pensions Regulator.

Railway Pension Investments

Based predominately at the London site, Railway Pension Investments Limited supports the 100-plus Railway employers sections within the RPS, and other schemes, in relation to investment management. It currently manages over £36.5bn of assets for the Scheme, and is one of the top ten largest pension funds in the UK in terms of assets under management. Railway Pension Investments Limited is the regulated FCA-authorised entity permitted to carry out certain regulated investment business under an Investment Manager Agreement with RPTCL.

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 Board of the Trustee Company comprises of 16 Non-Executive Directors, a third of whom retire by rotation every two years, with a six-year term of office.

Railpen Rail Operations looks after over

350,000

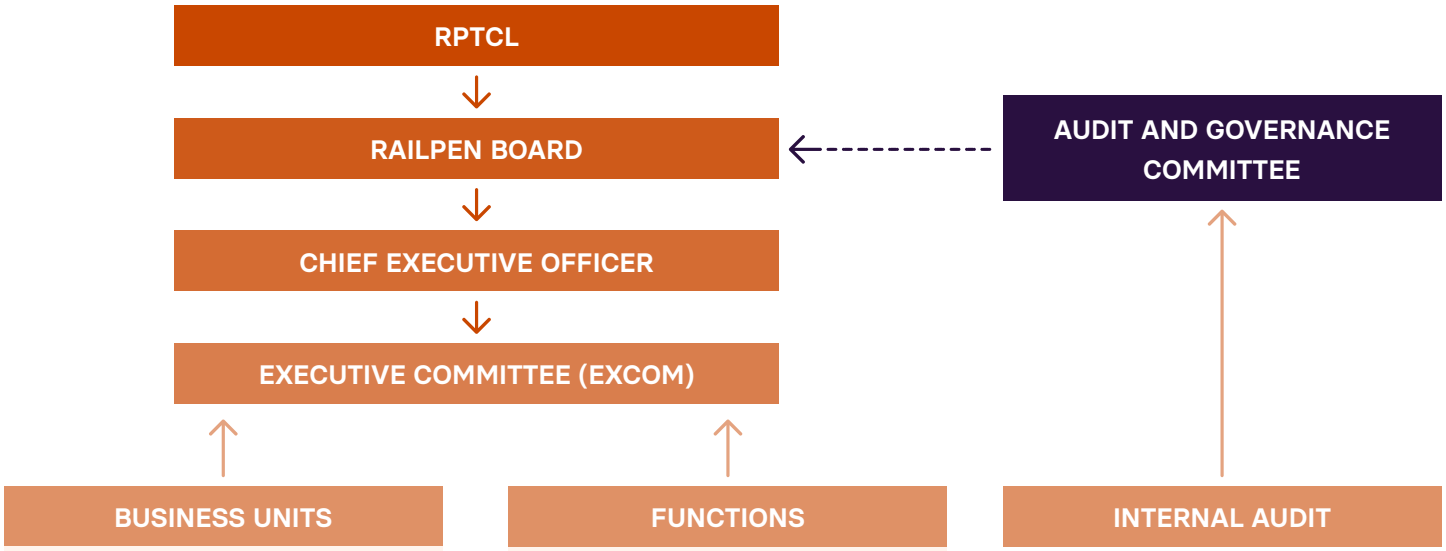
members in the Railway Pension Schemes

Railpen manages over

£36.5bn

in assets

ORGANISATION OVERVIEW



- Member Services
- Pensions and Investment Management

- Change and Transformation
- Corporate and Client Affairs
- Finance and Strategy
- People Team
- Legal and Company Secretariat
- Risk
- Technology, Security and Governance

Supporting Committees of the Trustee Company

Integrated Funding Committee

- Manages and agrees integrated funding plans for the railway 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 railway pension schemes, within the policy set by the Trustee Board, including the transfer value basis, Schedules of Contributions and recovery plans with sponsoring employers.
- Agrees section-specific valuation assumptions with sponsoring employers.
- Decides employer covenant categories and ratings for the purpose of actuarial valuations, and 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.

Member Casework and Administration Committee

- Considers and decides on the payment of benefits in all individual cases not delegated to Railpen or to a Pensions or Management Committee.
- Considers and decides on cases under the Internal Dispute Resolution procedure and Pensions Ombudsman cases.
- Agrees the terms of delegation to Railpen in respect of Trustee discretions under the Trust Deeds and Rules for schemes and sections without a Pensions or Management Committee.
- Oversees the delegation of benefit decisions to Pensions and Management Committees and review the consistency of decision-making across the railways pension schemes.
- Considers and decides on matters relating to any impact on members' benefits arising from operational rectifications.
- Clarifies the correct interpretation of scheme rules to direct Railpen in the accurate administration of members' benefits.
- Oversees and recommends Railpen's proposed service proposition and performance measures for approval by the Trustee Board.
- Oversees delivery of Railpen's administration services, including approval of disclosure and reporting requirements, and receives regular reports on administration performance.
- Oversees core scheme communications and considers member insights and feedback on member behaviours.
- Approves the Member Engagement Strategy and monitors its delivery.
- Monitors key scheme risks relating to pensions administration, including setting key risk indicators for inclusion in the Trustee's Risk Register.

Defined Contributions Committee

- Ensures the Trustee's Defined Contribution (DC) arrangements are appropriately managed and governed, including ongoing compliance of the IWDC Section with Master Trust authorisation criteria.
- Decides and monitors changes to employers' DC 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.
- Reviews the level of member-borne charges and fund transaction costs.
- Prepares an annual Chair's statement on governance, in line with regulations, and recommends it to the Trustee Board for approval.
- Considers aspects of the operation of the DC arrangements which contribute to value for members and assesses the level of value for members achieved.

Audit and Risk Committee

- Recommends for approval by the Trustee Company the appointment of the external auditor, the scope and planned programme of work and evaluates their effectiveness.
- Reviews all aspects of the annual accounts of Railtrust Holdings Ltd, the Trustee Company, railway pension schemes and pooled funds, and satisfies itself that they meet all relevant statutory requirements and professional standards.
- Recommends the accounts of Railtrust Holdings Ltd, the Trustee Company, and the railway pension schemes for approval by the relevant Boards.
- Approves the Pooled Fund Accounts.
- Is consulted on the scope and planned programme of work of Internal Audit and receives periodic reports on the progress against the Internal Audit annual plan and key Internal Audit findings.
- Responsible for the oversight of, and receives periodic reports on, the Trustee and Scheme risks.
- Reviews the Enterprise Risk Governance Framework and Enterprise Risk Policy on an annual basis.
- Receives annual reports from the Internal Audit team, and external auditors, regarding the operation of the Enterprise Risk Governance Framework and internal control systems, or any other relevant matters.

Railpen Board

The Railpen Board is responsible for the approval and ongoing monitoring of business strategy, financial performance, monitoring client delivery and ensuring we meet legal and regulatory requirements.

The Board comprises of Trustee Non-Executive Directors, independent Non-Executive Directors and two Executive Directors, including the Chief Executive. It operates with two business units: (1) Member Services and (2) Pensions and Investment Management. These business units are supported by our seven functions: Change and Transformation, Corporate and Client Affairs, Finance and Strategy, People Team, Legal and Company Secretariat, Risk and Technology, Security and Governance. Our Internal Audit team provides independent oversight over Railpen's control framework.

As a business we continue to enhance our technology and the administrative platforms we use as part of our long term plan to invest in Railpen and support our overarching vision to secure our members' futures.

Inevitably as our business changes shape and focus, our people, resources and structure will need to evolve to support it. The ExCom provides leadership, aligns decision-making across the business and oversees performance against the Railpen strategy. To aid the speed of decision-making and drive greater accountability, leadership groups operate to support each area.

Audit and Governance Committee

The Audit and Governance Committee (AGC) provides the Board with assurance on the effectiveness of the internal control and the governance framework. The Committee is accountable to the Board.

The AGC's responsibilities include:

- Approving, monitoring progress and reviewing the output of the Internal Audit annual plan.
- Overseeing business-wide processes, systems and controls.
- Overseeing the development and effectiveness of the corporate governance framework.
- Recommending for approval the accounting principles, policies and practices adopted in the preparation of the annual Railpen accounts.
- Recommending the Railpen Limited and Railway Pension Investments Limited accounts for approval to the Board.
- Receiving reports on whistleblowing and approving the Whistleblowing Policy.

Railpen Enterprise Risk Committee

The Railpen Enterprise Risk Committee (RERC) reports to the Railpen Board.

The RERC is responsible for oversight and monitoring of all enterprise and operational risk for the business.

The RERC's specific duties include the following:

- Approving the Enterprise Risk Governance Framework and Enterprise Risk Policy.
- Overseeing the effectiveness of the Enterprise Risk Governance Framework.
- Recommending for approval the Railpen risk appetite.
- Overseeing emerging risks.
- Receiving and reviewing reports from the Chief Risk and Compliance Officer.

Enterprise risk management

Managing risk is essential to an effective control framework. Our Enterprise Risk Governance Framework operates across all levels of the organisation with a dedicated Enterprise Risk Team overseeing robust governance including:

- An Enterprise Risk Governance Framework that defines the structure of the governance surrounding the management of enterprise risk and internal controls.
- An Enterprise Risk Policy that defines the guiding principles and framework for the management of enterprise risk.
- An Enterprise Risk Management Directive that documents the management practices and framework for the management of enterprise risk and provides the basis for measuring, controlling, monitoring and reporting risk across the business.

The Enterprise Risk Policy is reviewed regularly by management and annually by the Railpen Board and provides a framework for managing risk on a day-to-day basis. The Policy covers all aspects of operations for the Trustee Company and its subsidiaries.

Risk identification, assessment and management

Risks are identified and regularly reviewed by management and Directors through the risk management system which is updated regularly. Risks are evaluated by considering the likelihood of occurrence and the significance of the consequent impact on the business if they occur.

Each 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 enterprise risks are recorded in a specific Risk Register stored within the risk management system, which provides a means of regularly reviewing the assessment of each risk.

The Risk Registers identify the following for each risk:

- A risk ExCom owner who has overall responsibility for the risk.
- A risk owner responsible for managing the risk on a day-to-day basis.
- Key controls operating to mitigate the risk.
- An impact and likelihood assessment of the inherent, residual and target risk.
- An assessment of the current status of these measures.

The three lines of defence

The overall approach is based upon the 'three lines of defence' model as outlined below.

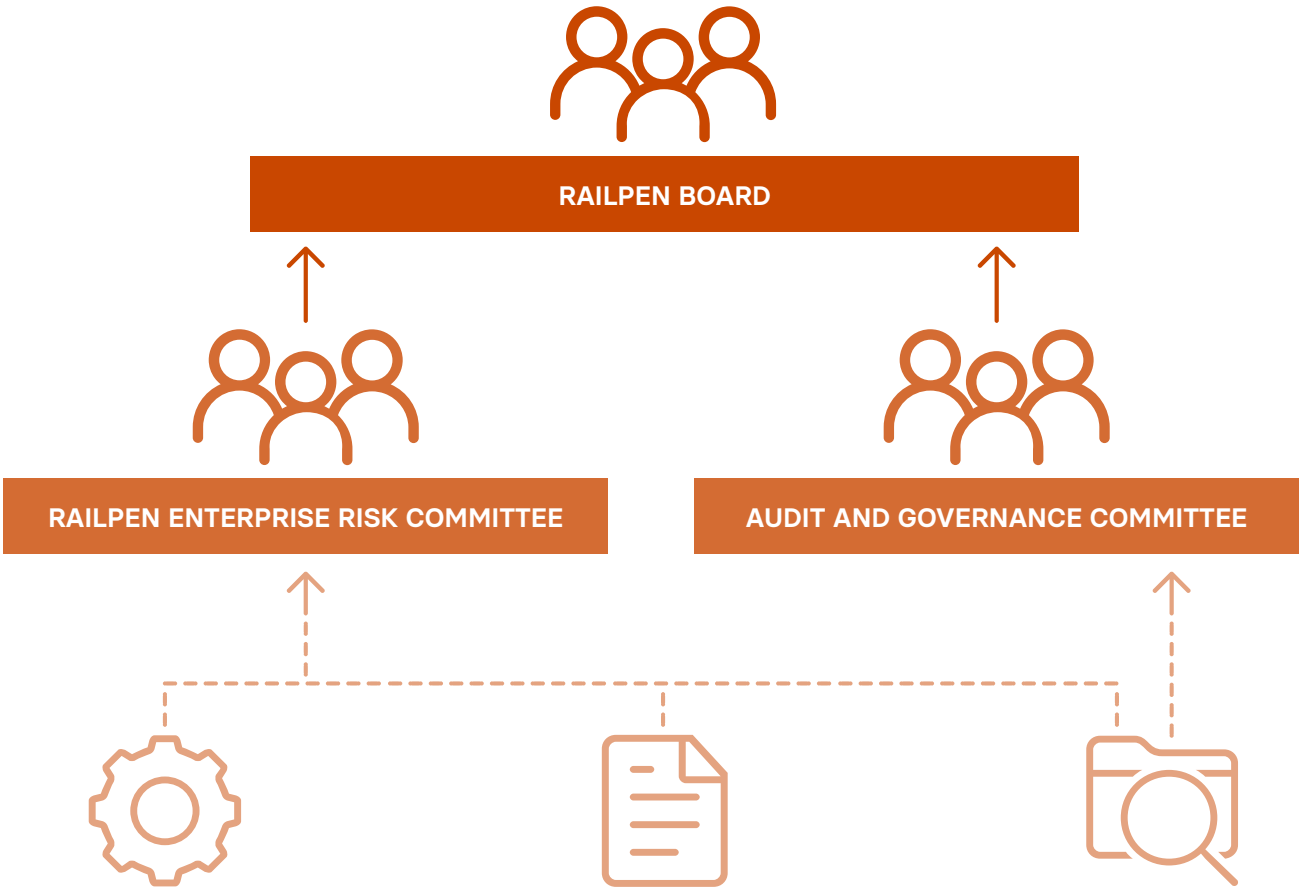
First line of defence:
This refers to the day-to-day controls that have been designed into systems and processes and the line management and supervision that ensures compliance and identifies breakdowns or other unexpected events or errors. These processes are supported by documented policies and procedures, or in some cases specific projects. Everyone is responsible for managing risk at Railpen.

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. The second line is reinforced by the monitoring functions of enterprise risk management through the Executive Risk Committee, Risk Managers and the Compliance team. The Data Protection team also sits within the second line.

Third line of defence:
This describes the independent assurance provided by Internal Audit, 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 role is to provide assurance and ensure the first two lines are operating effectively. Tasked by, and reporting to the Board and Audit and Governance Committee, it provides an evaluation of the effectiveness of governance, risk management and internal control to the governing body and senior management.

THE THREE LINES OF DEFENCE MODEL



FIRST LINE OF DEFENCE

- Management controls
- Day-to-day management of risk
- Policies and procedures

SECOND LINE OF DEFENCE

- Compliance
- Information Security
- Enterprise Risk Management
- Committees and Boards
- Data Protection

THIRD LINE OF DEFENCE

- Internal Audit
- External Audit

Internal Audit

Internal Audit services, overseen by the Chief Internal Auditor, are provided in-house by a dedicated team, including professionally qualified individuals. Through the delivery of internal audit and consulting services, 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.

Internal Audit governs itself by adherence to the Institute of Internal Auditors' 'Code of Ethics', and the Institute's 'Global Internal Audit Standards' constitute the operating procedures for Internal Audit.

The Internal Audit function is independent of operational management. While the Chief Internal Auditor reports administratively to the Chief Financial Officer, functional reporting is to the Audit and Governance Committee and the Trustee Audit and Risk Committee. The function has unrestricted access to the Chief Executive Officer, the Chairs of the Audit and Governance Committee and the Trustee Audit and Risk Committee, and, where necessary, the Board Chairs, supporting independent judgement and objective assurance.

Authority is granted for full, free and unrestricted access to any and all of the records, physical properties, and personnel relevant to any function under RPTCL and its operating companies.

The mandate of Internal Audit is represented in the Internal Audit Charter, which is subject to approval by the Audit and Governance Committee on at least an annual basis.

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 company objectives. The planning process involves:

- Understanding the strategy and business objectives.
- Identification of key risks and controls associated with each area.
- Reviewing 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 reviewed throughout the year to ensure its ongoing alignment, and is formally approved by the Audit and Governance Committee.

Information security

Railpen has established a formal information security governance framework aligned to recognised industry standards and best practice. The organisation maintains certification to ISO/IEC 27001, providing independent assurance that an effective information security management system is in place and operating.

Overall accountability for information security governance and internal control is assigned to the Chief Information Security Officer. Responsibilities are supported by approved policies, standards and procedures which define how information security risks are identified, managed and monitored.

Employee responsibilities for the secure use of information and systems are defined within the IT Acceptable Use Policy. This operates alongside a GDPR compliant Data Protection Policy and is reinforced by physical and logical access controls. These controls collectively provide a framework for protecting employer, member and partner data.

The IT Acceptable Use Policy sets out specific requirements covering internet and email usage, social media, system access, data protection, remote working and the use of mobile devices. Compliance with these requirements is mandatory for all employees and relevant third parties.

Railpen operates a layered security approach ("defence in depth") that incorporates preventative, detective and corrective controls to reduce the likelihood and impact of security incidents.

The IT infrastructure is monitored on a continuous basis using a combination of IT and cyber security monitoring tools, enabling timely identification and response to security events or system issues.

The effectiveness of information security controls is subject to regular assessment. This includes internal audit activity, independent external security reviews and testing designed to reflect current and emerging cyber threats. Annual cyber security exercises are carried out to test incident response arrangements, roles and responsibilities, and the effectiveness of documented procedures.

Railpen maintains ongoing security awareness and training programmes, supported by continuous professional development for IT and security personnel. Security technologies, tools and controls are regularly reviewed and enhanced to address changes in the threat landscape and to ensure continued effectiveness.

Business Continuity

Railpen's Business Continuity is co-ordinated by the Chief Technology Officer and Chief Information Security Officer and delivered by the Business Continuity and Resilience Manager. A full business continuity and disaster recovery process along with supplemental business area plans are in place. Resilience is the core principle to our architecture design. Our resilient architecture means we operate from a third party privately managed cloud spanning across two Tier 4 data centres located in separate geographic areas, enabling full failover, which enables our staff to continue to work remotely in the event of a disruption.

Ransomware remains one of the top cyber risks that could disrupt normal operations, and we have many layers of security in place to prevent, detect and respond to such an event, including an immutable backup vault solution, enabling us to fully recover our systems and data.

The scope of the Business Continuity Management System (BCMS) covers the entire business. Roles and responsibilities are assigned, with the business executives having overall business continuity accountability.

The holistic scope of business continuity also includes Railpen crisis and incident management which ensures synergy between our planning, preparedness, and protective capabilities. Railpen business continuity is configured to the principles of ISO 22301, which underpins our ISO 27001 certification.

Railpen confirms that similar effective business continuity controls are in place for the core pension administration system supporting the schemes' members. This system is hosted by our supplier. The system is replicated across two data centres, and tests are carried out on an annual basis.

Safeguarding assets

There are a number of measures that we adopt to protect Railpen'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, record-keeping and reconciliation.

The Financial Crime team owns Railpen's Anti-Fraud Policy and Response Plan, ensuring that management is well prepared to deal with any fraud incidents efficiently and effectively.

Being committed to high standards of openness, probity and accountability, we have prepared a Whistleblowing 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 Railpen 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 we operate in accordance with relevant pension regulations and legislation, Railpen has a dedicated Technical team. The team supports Railpen and the Trustee in providing pensions administration services which are legislatively and regulatory compliant. 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. The team issue regulatory updates, host briefing sessions and support the business through any change required.

The team support the ongoing Pensions Regulator supervision to our Master Trust arrangement and also support the administration teams to provide an accurate and effective administration service in line with the relevant trust deeds and rules.

Staff training and development

At Railpen, 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 HR 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. This involves setting accountabilities, priorities and expected behaviours through our Job on a Page process. Regular performance conversations take place throughout the year to review progress; leading to a final annual review.

Railpen is dedicated to providing employees with training and development that ensures the achievement of Railpen objectives and strategy. We encourage training that best fits their role or other relevant professional accreditations including QPA and PMI (Pensions Administration), ACA, ACCA and CIMA (Accounting), CIM (Marketing), PRINCE 2 (Project Management) and MCSE (IT).

STATEMENT OF INTERNAL CONTROLS

This section contains the statement of internal controls for Railpen for the year ended 31 December 2025.

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 01/20.

All tests of operating effectiveness of internal controls were undertaken for the period ended 31 December 2025.

Control objectives

Pensions Administration

1. **Accepting clients**
   - New client agreements and amendments are authorised prior to initiating pension administration activity.
   - Pension scheme member details and accounts are completely and accurately set up onto relevant systems in accordance with the scheme rules and individual elections.
   - Opening balances for client take-ons are completely and accurately recorded and communicated to clients in line with client instructions.
2. **Authorising and processing transactions**
   - Contributions and transfers-in received, and where applicable allocations of members' funds to investment options are processed completely, accurately and within agreed timescales.
   - Switches of members' funds between investment options and other rebalancing transactions are processed completely, accurately and within agreed timescales.
   - Benefits payable and transfer values are calculated in accordance with scheme rules and relevant legislation and are paid within agreed timescales.
3. **Maintaining financial and other records**
   - Member records consist of up-to-date and accurate information.
   - Requests to change member records are validated for authenticity.
   - Contributions and benefit payments are completely and accurately recorded in the proper period.
   - Investment transactions, balances and related income are completely and accurately recorded in the proper period.
4. **Safeguarding assets**
   - Member records are securely held and access restricted to authorised individuals.
   - Cash in scheme bank accounts is safeguarded and payments are suitably authorised.
5. **Managing and monitoring compliance and outsourcing**
   - Receipt of contributions, in accordance with timescales, scheme rules and legislative requirements are monitored.
   - Pension administration activities are governed by service level agreements that are authorised and subject to regular review. Service performance is regularly monitored and assessed against the standards set out in service level agreements.

- Transaction errors are identified, reported to clients and resolved in accordance with established policies.
- Periodic reports to The Pensions Regulator and HMRC are complete and accurate.

6. Reporting to clients

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

Information Technology

7. Restricting access to systems and data

- Physical access to in-scope systems is restricted to authorised individuals.
- Logical access to in-scope systems and data is restricted to authorised individuals in accordance with job roles and/or business requirements.
- Client and third party access to in-scope systems and data is restricted and/or monitored.
- Segregation of incompatible duties within and across business and technology functions is formally defined, implemented, updated and enforced by logical security controls.

8. Maintaining integrity of the systems

- Scheduling and internal processing of data is complete, accurate and within agreed timescales.
- Transmission of data to/from external parties is complete, accurate, executed within agreed timescales and secure in line with external party agreements.
- Network perimeter security devices are installed and changes are tested and approved.
- Anti-virus definitions are periodically updated across all terminals and servers, deployment and settings are periodically reviewed and updated when required; and patterns of attempted external breaches are monitored.
- Data received from external parties is scanned for known vulnerabilities, any compromised data is quarantined and definitions of threats are periodically updated.

9. Maintaining and developing systems hardware and software

- Development and implementation of both in-house and third party in-scope systems are authorised, tested and approved.
- Data migration or modification is authorised, tested and, once performed, reconciled back to the source data.
- Changes to existing in-scope systems, including hardware upgrades, software patches and direct configuration changes, are authorised, tested and approved in line with policy.

10. Recovering from processing interruptions

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

11. Managing and monitoring compliance and outsourcing

- Outsourced activities provided by Subservice Organisations are governed by contracts and service level agreements that are authorised and subject to regular review.
- The services provided by Subservice Organisations are regularly monitored and assessed against the standards set out in the service level agreements.

Summary of controls tested

Pensions Administration

Title	Controls	Pages	Summary of results
Accepting clients	10	19-22	No exceptions
Authorising and processing transactions	22	23-32	1 exception
Maintaining financial and other records	16	33-39	No exceptions
Safeguarding assets	9	40-43	1 exception
Managing and monitoring compliance and outsourcing	14	44-49	No exceptions
Reporting to clients	6	50-51	No exceptions

Information Technology

Title	Controls	Pages	Summary of results
Restricting access to systems and data	16	52-57	2 exceptions
Maintaining integrity of the systems	19	58-64	1 exception
Maintaining and developing systems hardware and software	8	65-68	No exceptions
Recovery from processing interruptions	14	69-74	2 exceptions
Managing and monitoring compliance and outsourcing	4	75-76	No exceptions

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.
- 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 **77**

Information Technology **61**

PENSIONS ADMINISTRATION

1. Accepting clients

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

All new sections or categories of membership are subject to formal approval on behalf of the Trustee by the Integrated Funding Committee (IFC) or the Defined Contribution Committee (DCC).

Rule amendments and participation deeds are executed on behalf of the Employer and the Trustee. This process is supported by the in-house Pensions Policy and Legal teams and documents are signed prior to live administration.

No.	Detailed controls	Relevant exceptions 'if any'	DB	DC
1.1	New shared cost sections or changes to member benefit structures require approval through the IFC. New employers to the IWDC section require approval of the DCC unless the employer already participates in the scheme through the shared cost arrangement. The IFC and DCC are delegated sub-committees of the Trustee.	**Inspection** Confirmed by inspection for a sample of new section set-ups or amendments to member benefit structures that approval was required from IFC.** Confirmed by inspection for a sample of new employers to the IWDC Section that approval from the DCC was documented unless the employer already participated in the scheme through the shared cost arrangement.** **Control not able to be applied.**	●	●
1.2	Deeds of participation for new employers and deeds of amendment to the rules for existing sections are appropriately executed on behalf of the Trustee (and Pension Committee where there is one) and the relevant employer before the rule is effected.	**Inspection** Confirmed by inspection for a sample of new employers and amendments to existing sections that deeds were appropriately executed on behalf of the Trustee (and Pension Committee where applicable).** **No exceptions to the company's procedures were noted.**	●	●

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

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

A cross functional implementation team is established to deliver a new section or category of membership. A standard project plan provides the basis for the process. A Project Manager oversees progress of the plan and the Client Relationship Manager (CRM) responsible for the section is an active participant in the process.

Where major benefit reforms are implemented, a standard scheme benefits schedule, detailing the design of the section, is created by the Railpen Pensions Policy and Technical team based on the deed of amendment and is verified by the client.

Calculation specifications are updated and approved by the Technical team. All potential scheme elections within the scheme rules are contained within a reference data library. Testing is carried out on elections in a test environment, only being implemented into the live administration platform once formally approved. First occurrence validations of calculations are performed in the live environment post implementation to confirm the effectiveness of the change.

No.	Detailed controls	Relevant exceptions 'if any'	DB	DC
1.3	An implementation team, with cross functional representation, is established to undertake a standard section set-up. Key milestones within the plan are agreed with the client and monitored through CRM project reporting.	**Inspection** Confirmed by inspection for a sample of new section set-ups that an implementation team had been established and that project milestones were agreed with the client and were monitored through CRM project reporting.** **Control not able to be applied.**	●	●
1.4	Where major benefit reforms are implemented a standard scheme benefits schedule is created by Railpen and verified by the client to agree and understand all aspects of benefit design.	**Inspection** Confirmed by inspection for a sample of major benefit reforms that a standard benefit schedule was created by Railpen and verified by the client.** **Control not able to be applied.**	●	
1.5	Scheme actuaries provide instructions for the benefit calculation methodology and factors, where these are required, as part of the new section set-ups.	**Inspection** Confirmed by inspection for a sample of new section set-ups that actuarial instructions had been received for benefit calculation methodology and factors where required.** **Control not able to be applied.**	●	

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

No.	Detailed controls	Relevant exceptions 'if any'	DB	DC
1.6	Calculation specifications are updated by the Technical team and tested prior to implementation within the system.	**Inspection** Confirmed by inspection of sample of updated calculation specifications that these had been created by the Technical team and had been tested and reviewed prior to implementation.** **No exceptions to the company's procedures were noted.**	●	
1.7	A data library is maintained which lists all potential scheme elections within the confines of the scheme rules. The scheme elections are input into a test environment, checked and approved before implementation into live.	**Inspection** Confirmed by inspection that a data library was maintained and added to with changes and additions to reference data for sections and employers.** Confirmed by inspection that any changes and additions had been input into a test environment, checked and approved before implementation into live.** **No exceptions to the company's procedures were noted.**	●	●
1.8	For a new scheme set-up, or changes to benefit provision, the first occurrences of calculations are reviewed for accuracy by a technical expert. Where required, the first occurrence of calculations are referred to the scheme actuary for review.	**Inspection** Confirmed by inspection for a sample of first occurrence calculations that they had been reviewed for accuracy by a technical expert and where required, the scheme actuary had completed a review.** **Control not able to be applied.**	●	●

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

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

Opening balances are only relevant for TUPE transfers to a new section or category. Automated routines are available for processing TUPE transfers, however where manual updates are required, an instruction detailing the set-up requirements based on member elections is loaded into a test environment. Once review and authorisation stages are complete the data is loaded into the live environment and the member is notified that the transfer is complete.

No.	Detailed controls	Relevant exceptions 'if any'	DB	DC
1.9	Member opening unit balances, service credits and earliest benefits dates relating to TUPE transfers to a new section or category, are applied using automated routines. Where manual updates are required, these are input into a test environment and are subject to review and authorisation prior to upload to the live environment.	**Observation** Confirmed by observation that TUPE transfers were applied using automated routines.** **Inspection** Confirmed by inspection for a sample of for a manual TUPE transfers where applicable, that new or amended member records were subject to review in a test environment and were authorised for upload to the live environment.** **No exceptions to the company's procedures were noted.**		●
1.10	Records are updated based on member elections and are confirmed to the member once the TUPE has completed.	**Inspection** Confirmed by inspection for a sample of members within a TUPE transfer that records were updated in line with member elections and the member was notified once the TUPE was completed.** **No exceptions to the company's procedures were noted.**		●

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

2. Authorising and processing transactions

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

Contributions are paid in accordance with a schedule of contributions determined for each scheme with contributing members. The schedules are monitored against the scheme rules (7 days after pay date) and regulatory requirements, 22nd of the subsequent month if paying electronically. Sponsoring employers receive reminders on the employer portal with regards to their contribution deadlines.

Escalation routines involving the Trustee, CRM and ultimately the regulator, are in place to ensure member contributions are collected accurately and invested in a timely manner.

Data files are received from employers detailing contributions by employer and member. These files are uploaded onto the administration system though 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. Validation failures must be resolved prior to the data being accepted on to the system.

Schedules of expected contributions are in place and a segregation exists between the Employer Support team, supporting the processing of the data files on the administration system and the Finance team entering the cash received.

DC and AVC contributions and transfers-in 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). The Investment Manager instruction is processed via an automated gateway where the Investment Manager updates unit holdings and prices automatically on a daily basis.

Regular unit reconciliations are undertaken to ensure that the units recorded by the Investment Manager agree to the units in the administration system. Any discrepancies are corrected as appropriate.

Timely processing of transfer-in cases is monitored in line with agreed service levels through system-produced automated management information and workload management processes.

No.	Detailed controls	Relevant exceptions 'if any'	DB	DC
2.1	Data is subject to automated formatting rules and data validation steps in line with scheme rules and legislation.	**Observation** Confirmed by observation that contribution files and individual data submissions were subject to automated format and scheme validation and schedules were fully reconciled.** **No exceptions to the company's procedures were noted.**	●	●

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

No.	Detailed controls	Relevant exceptions 'if any'	DB	DC
2.2	The Employer Support team maintain daily oversight of contribution schedules. Daily exception reporting is reviewed to ensure issues identified are addressed within agreed timescales.	**Inspection** Confirmed by inspection for a sample of days that daily exception reports had been produced and reviewed with appropriate action taken to resolve issues identified within agreed timescales.** **No exceptions to the company's procedures were noted.**	●	●
2.3	Contribution schedules are made available to employers via the employer portal prior to pay date to allow accuracy of data held by Railpen to be confirmed in advance.	**Observation** Confirmed by observation of the employer portal that contribution schedules were available to view prior to submission.** **No exceptions to the company's procedures were noted.**	●	●
2.4	Contributions are allocated to the correct investment products based on scheme and members' allocation requirements using automated routines.	**Observation** Confirmed by observation of the process, that automated routines were used to allocate the contributions to the correct investment product based on the scheme or member requirements.** **Inspection** Confirmed by inspection for a sample of contributions received that investments had been made in accordance with the allocation requirements and that member records had been updated.** **No exceptions to the company's procedures were noted.**		●

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

No.	Detailed controls	Relevant exceptions 'if any'	DB	DC
2.5	Scheme parameters determine if the scheme permits transfers-in. Transfers-in are allocated to the correct investment products based on scheme and members' allocation requirements using automated routines.	**Observation** Confirmed by observation of the process, that automated routines were used to allocate the transfers to the correct investment product based on the scheme or member requirements.** **Inspection** Confirmed by inspection that there had been no transfers-in to schemes that did not permit new members.** Confirmed by inspection for a sample of transfers-in received that investments had been made in accordance with the allocation requirements and that the members record had been updated.** **No exceptions to the company's procedures were noted.**	●	●
2.6	Transfer-in charge instructions created within the administration system must reconcile to cash received in order for the transfer to successfully complete. Any discrepancies outside of agreed tolerance are investigated.	**Inspection** Confirmed by inspection for a sample of transfers-in that the amount received agreed to the change instruction and member correspondence. Confirmed that any discrepancies outside of agreed tolerances were resolved prior to the transfer completing.** **No exceptions to the company's procedures were noted.**	●	●
2.7	Transfers-in are monitored for timely completion through workload management processes. Team managers utilise system-produced management information to allocate casework and review existing workloads on a daily basis. Transfer-in payments are monitored using a tracker to ensure payments received are reconciled in a timely manner.	**Observation** Confirmed by observation that transfers-in were monitored for completion in accordance with agreed timescales through the workload management process.** **Inspection** Confirmed by inspection that a Transfer-in payment tracker was maintained and reconciliations were completed in a timely manner.** **No exceptions to the company's procedures were noted.**	●	●

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

No.	Detailed controls	Relevant exceptions 'if any'	DB	DC
2.8	Regular reconciliations are performed at a fund level to ensure the units recorded in the administration system agree with the units held by the Investment Manager with issues noted and resolved.	**Inspection** Confirmed by inspection for a sample of schemes, that unit reconciliations were carried out between the units held by the Investment Manager and those recorded in the pensions administration system.* **Observation** Confirmed by observation that where issues were noted these were resolved.* **No exceptions to the company's procedures were noted.**		●

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

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.

The Member Services Change and Delivery Committee oversees the cyclical event process including rebalancing transactions. Lifestyle profiles are built into the administration system in order to enable automated lifestyle investment switches.

No.	Detailed controls	Relevant exceptions 'if any'	DB	DC
2.9	Transfers between investment options including lifestyle switches are allocated to the correct investment products based on scheme and members' allocation requirements using automated routines. The member portal has a direct interface with the administration system. Where manual updates are required, member authorisation is obtained via an approved form.	**Observation** Confirmed by observation of the process, that automated routines were used to allocate switches to the correct investment product based on the scheme or member requirements and where manual processing had taken place a review had been undertaken.** **Inspection** Confirmed by inspection for a sample of manual switches that member authorisation had been received via an approved from, investments had been made in accordance with the allocation requirements, and that the member record had been updated.** **No exceptions to the company's procedures were noted.**		●

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

No.	Detailed controls	Relevant exceptions 'if any'	DB	DC
2.10	Switches are monitored for timely completion through workload management processes. Team managers utilise system-produced management information to allocate casework and review existing workloads on a daily basis.	**Observation** Confirmed by observation that switches were monitored for completion in accordance with agreed timescales through the workload management process.** **No exceptions to the company's procedures were noted.**		●
2.11	Rebalancing transactions form part of the cyclical event process overseen by the Member Services Continuous Improvement Forum and are conducted on a quarterly basis unless a deviation is agreed by senior management. The automated process produces exception reports which are reviewed and appropriately actioned.	**Inspection** Confirmed by inspection that rebalancing transactions formed part of the cyclical event process overseen by the Member Services Continuous Improvement Forum which was conducted quarterly unless a deviation was agreed by senior management.** Confirmed by inspection for a sample of exception reports that these were reviewed and action was taken where necessary.** **No exceptions to the company's procedures were noted.**		●

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

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

The Member Services Continuous Improvement Forum monitors legislative and regulatory developments which may impact the payment of benefits and ensures these are identified and systems and processes updated accordingly.

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 tested prior to upload to the live system and manual calculation tools. A record is kept as a clear audit trail.

System based routines are used to identify members with flexible benefits 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 employer provided information to ensure that calculations are accurate.

A suite of reconciliation reports is generated as part of the payroll closedown routine. The payroll is again reconciled and discrepancies resolved in advance of payment.

Payments are reviewed for accuracy and the payroll is approved by an appropriately authorised team member before it is issued for payment by the internal BACS Bureau.

Transfers-out are calculated using automated workflows. Key documentation is required for a member to transfer out of a scheme including signed indemnity and discharge forms. Appropriate due diligence is performed on all transfers-out, suspect cases are escalated accordingly, and where necessary, Action Fraud is notified to assist in the prevention of Pension Liberation Fraud. Transfers exceeding agreed criteria are subject to additional oversight from the Technical team and scheme actuary, where necessary.

No.	Detailed controls	Relevant exceptions 'if any'	DB	DC
2.12	A Member Services Continuous Improvement Forum exists to monitor and ensure regulatory and legislative changes are identified and associated changes implemented effectively.	**Inspection** Confirmed by inspection for a sample of months that regulatory and legislative changes had been considered by the Member Services Continuous Improvement Forum and action taken where required.* **No exceptions to the company's procedures were noted.**	●	●

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

No.	Detailed controls	Relevant exceptions 'if any'	DB	DC
2.13	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 by inspection for a sample of benefits calculated, that automated routines were used. Where this was not possible, confirmed that a manual calculation had been subject to secondary review.* **No exceptions to the company's procedures were noted.**	●	●
2.14	Routine benefit payments in respect of retirements are paid in line with member retirement options. Retirements are monitored for timely completion through workload management processes.	**Inspection** Confirmed by inspection for a sample of retirements that documentation had been received from the member and that payment was made in line with member choices.* **Observation** Confirmed by observation that retirements were monitored against agreed timescales through the workload management process.* **No exceptions to the company's procedures were noted.**	●	●
2.15	Benefit payments in respect of death lump sums are reviewed and approved through the appropriate committee or through delegated authority. Death lump sum payments are monitored for timely completion through workload management processes.	**Inspection** Confirmed by inspection for a sample of death lump sum benefits that the case had been appropriately reviewed and approved in line with delegations.* **Observation** Confirmed by observation that death lump sums were monitored against agreed timescales through the workload management process.* **No exceptions to the company's procedures were noted.**	●	●

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

No.	Detailed controls	Relevant exceptions 'if any'	DB	DC
2.16	Parameter updates are applied using client authorised sources, including government indices and scheme actuary notifications. Changes are applied and tested in a test environment before being applied into both the live system and associated manual calculation tools. All changes are subject to secondary review.	**Inspection** Confirmed by inspection for a sample of parameter changes that an authorised source was used and the system and manual calculation tools were tested and reviewed prior to being updated.** Confirmed by inspection for a sample of changes that they are subject to secondary review.** **No exceptions to the company's procedures were noted.**	●	●
2.17	System based routines are used to identify members with flexible benefits approaching retirement age. Members are contacted within agreed timescales with retirement options.	**Observation** Confirmed by observation that system based routines were used to identify members with flexible benefits approaching retirement age.* **Inspection** Confirmed by inspection for a sample of members approaching retirement age that they were contacted within agreed timescales with retirement options.* **Exception** Wake-up letters were not issued during the period to some members of the RPS DB scheme with additional voluntary contributions. **Management response** The wake-up letter process has been reviewed simplified and training has been provided. Additional measures have been put in place to ensure there is effective oversight of the end-to-end process and confirmation of distribution is evidenced. We will review and reissue those letters where members have not yet accessed their benefits.	●	●

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

No.	Detailed controls	Relevant exceptions 'if any'	DB	DC
2.18	Transfers are calculated and processed via automated workflows and are guaranteed and paid in accordance with legislative timescales. Where manual calculations are required they are subject to secondary review.	**Inspection** Confirmed by inspection for a sample of transfers that automated workflows had been used and transfers were accepted and paid within guaranteed timescales. Where automation was not possible, confirmed that a manual calculation had been subject to secondary review.** **No exceptions to the company's procedures were noted.**	●	●
2.19	Checklists exist to ensure appropriate due diligence is carried out on transfers in accordance with regulations. Suspect cases are raised with the Technical team who would consider the case for reporting to The Pensions Regulator/Action Fraud helpline.*	**Inspection** Confirmed by inspection for a sample of transfers that appropriate due diligence was carried out and where applicable, suspect cases were escalated accordingly.** **No exceptions to the company's procedures were noted.**	●	●
2.20	Material transfers meeting client agreed criteria are subject to additional oversight. Where necessary, the case is escalated to the scheme actuary.	**Inspection** Confirmed by inspection for a sample of transfers meeting the established client criteria, that additional reviews had been undertaken and that the calculations had been referred to the scheme actuary as appropriate.** **No exceptions to the company's procedures were noted.**	●	
2.21	Payrolls are paid in accordance with agreed timetables contained within the administration system. Regular oversight meetings ensure the process is closely monitored.	**Inspection** Confirmed by inspection for a sample of payrolls that an oversight meeting took place and payrolls were made in accordance with agreed timescales.* **No exceptions to the company's procedures were noted.**	●	

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

No.	Detailed controls	Relevant exceptions 'if any'	DB	DC
2.22	Payroll closedown routines ensure all exceptions have been addressed prior to the creation of the payroll file. Once finalised the payroll is authorised by an approved payroll administrator.	**Inspection** Confirmed by inspection for a sample of payrolls that balancing and reconciliation reports had been reviewed for exceptions and action taken to resolve these prior to the payroll being authorised by an approved payroll administrator.* **No exceptions to the company's procedures were noted.**	●	

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

3. Maintaining financial and other records

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

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 The Pensions Regulator guidance on measuring member data ('common data' requirements).
- UK pensioner existence checks using an external tracing bureau and case reviews to confirm legitimacy of certain benefit types.

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 through the employer portal into the administration system following validation checks. Member data can also be updated using the secure member portal which requires a unique user login and password authentication.

All client communication requires authorisation from the client/member before amending member data. Member correspondence is scanned onto the member record on the administration system for reference.

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

No.	Detailed controls	Relevant exceptions 'if any'	DB	DC
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 by inspection for a sample of periods that UK pensioner existence checks had been undertaken, and action taken where appropriate.* **No exceptions to the company's procedures were noted.**	●	

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

No.	Detailed controls	Relevant exceptions 'if any'	DB	DC
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 by inspection for a sample of pensioners that existence checks/ case reviews were carried out, supporting documentation was obtained and where necessary, member payments were suspended.* **No exceptions to the company's procedures were noted.**	●	
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 respective governance forum and appropriate action taken.	**Inspection** Confirmed by inspection for a sample of schemes that member data was regularly reviewed in line with The Pensions Regulator guidance. Where discrepancies were identified they were escalated to the respective governance forum, and appropriate action was taken.* **No exceptions to the company's procedures were noted.**	●	●
3.4	The creation of new member records and member data changes, as advised by the scheme sponsor, are subject to automated validation prior to being processed in the system.	**Observation** Confirmed by observation that employer submissions were subject to automated validations.* **No exceptions to the company's procedures were noted.**	●	●

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

No.	Detailed controls	Relevant exceptions 'if any'	DB	DC
3.5	Member records are automatically updated using tax code information provided by HMRC. Where manual updates are required a work item is created and actioned.	**Inspection** Confirmed by inspection for a sample of automated cases that member records were accurately updated in line with information provided by HMRC. Where manual updates were required, a work item was created and actioned.* **No exceptions to the company's procedures were noted.**	●	
3.6	An annual exercise is undertaken to confirm and reconcile salary details provided by the sponsoring employers to those held within the administration system.	**Inspection** Confirmed for a sample of employers that salary data held in the administration platform was reconciled to that provided by the employer. Any differences were investigated and the system updated accordingly.* **No exceptions to the company's procedures were noted.**	●	

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

Requests to change member records are validated for authenticity.

Members and employers can update member records using a number of different methods, including both member and employer portals. Requests must pass through specific security validations before being applied into the live administration platform.

Certain benefit payments are subject to additional security measures to validate recipient details prior to payment.

No.	Detailed controls	Relevant exceptions 'if any'	DB	DC
3.7	Members can update and amend personal details via a secure member portal which is subject to initial registration and security validations prior to access.	**Observation** Confirmed by observation of the member portal that initial registration was required and security validations were in place which must be passed prior to accessing the site or updating and amending personal details.* **No exceptions to the company's procedures were noted.**	●	●
3.8	Employers are able to update and amend member records via a secure portal. Employers must pass portal security validations prior to accessing and uploading information.	**Observation** Confirmed by observation of the employer portal that security validations were in place which must be passed prior to accessing the portal or updating and amending personal details.* **No exceptions to the company's procedures were noted.**	●	●
3.9	Requests to change data must derive from an authorised source with sufficient information provided to allow validation and are only made following channel specific security validations.	**Observation** Confirmed by observation that changes to data must derive from an authorised source, channel specific security validations were in place and sufficient information was provided to validate a change.* **No exceptions to the company's procedures were noted.**	●	●
3.10	The details of recipients of certain payments are verified prior to payments taking place.	**Inspection** Confirmed by inspection for a sample of retirement and death lump sum payments that recipient details had been subject to verification, prior to payment taking place.* **No exceptions to the company's procedures were noted.**	●	●

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

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. Intraday data flows to and from the administration/accounting system.

Daily bank reconciliations are undertaken to ensure cash is accounted for accurately and in the correct period.

No.	Detailed controls	Relevant exceptions 'if any'	DB	DC
3.11	Scheme transactions input into the pensions administration system are imported into the accounting system intraday following validation and correction of any returned errors. An audit trail of changes to the file is produced and reviewed as part of the bank reconciliation process.	**Inspection** Confirmed by inspection 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.* **Enquiry** Confirmed by enquiry that the bank reconciliation process could only be completed once all changes had been reviewed and 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 by inspection for a sample of days that regular bank reconciliations were undertaken to ensure all cash movements were accounted for accurately in the proper period.* **No exceptions to the company's procedures were noted.**	●	●
3.13	Where daily banking checks identify discrepancies, these are placed into the suspense account, which is regularly monitored and items are appropriately cleared.	**Inspection** Confirmed by inspection that the suspense account is regularly reviewed to ensure items are being cleared appropriately.* **No exceptions to the company's procedures were noted.**	●	●

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

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

The administration system uses a routine to upload contributions, reference these to the particular member investment choice allocation and aggregate the nominal investment amount for each fund. The investment instruction is then sent to the Investment Manager (DC trading platform) 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 in the administration system. System generated unit data reports are compared to the Investment Manager statements at a fund level. Discrepancies of more than one unit are fully investigated and resolved.

Regular reviews of cash settlements ensure that all investment related income is identified and recorded appropriately on the date it is received.

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.

No.	Detailed controls	Relevant exceptions 'if any'	DB	DC
3.14	Regular reconciliations are performed at a fund level to ensure the units recorded in the administration system agree with the units held by the Investment Manager and issues noted are resolved.	**Inspection** Confirmed by inspection for a sample of schemes, that unit reconciliations were carried out between the units held by the Investment Manager and those recorded in the pensions administration system.* **Observation** Confirmed by observation that where issues were noted these were resolved.* **No exceptions to the company's procedures were noted.**		●
3.15	Cash Settlement Control reports produced from the account ledger highlight any trades that have any outstanding cash settlement outside of the standard two-day window.	**Inspection** Confirmed by inspection for a sample of Cash Settlement Control reports that trades which had any outstanding cash settlement outside of the standard two-day window were reviewed and reconciling items were investigated and cleared.* **No exceptions to the company's procedures were noted.**		●

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

No.	Detailed controls	Relevant exceptions 'if any'	DB	DC
3.16	Investment instructions provided to the investment manager use STP. The investment instruction is fully automated to ensure that funds are accurately updated.	**Inspection** Confirmed by inspection for a sample of investments made, that STP had been used for the investment instruction and the funds had been accurately updated.** **No exceptions to the company's procedures were noted.**		●

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

4. Safeguarding assets

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

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 an application level, access is split into distinct roles, each of which offers the user different abilities and access within the pensions administration platform. The role segregation is designed to ensure that logically incompatible activities are not available to a single group of users, and to protect the core function of the system from access by unauthorised individuals.

Secure portals are in place for members and employers which allow updates to records to be made, subject to registration and security validation steps. Access to employer portals is regularly reviewed and updated based on employer requirements.

No.	Detailed controls	Relevant exceptions 'if any'	DB	DC
4.1	Enforced network password security protocols are in place requiring users to adopt minimum complex character length and lock out after a number of unsuccessful attempts.	**Inspection** Confirmed by inspection of the network configuration that enforced password requirements were in place.* **No exceptions to the company's procedures were noted.**	●	●
4.2	Member and scheme data held on the administration system is restricted to authorised personnel across different access profiles.	**Inspection** Confirmed by inspection for a sample of users, that their administration access was appropriate to their role.* **Exception** In seven out of ten BaNCS profiles sampled, the user roles assigned did not map correctly to the documented user role profiles. **Management response** As part of our continual improvement activity new BaNCS role profiles have been introduced and all roles will have been reviewed against these profiles by the end of the July 2026 quarterly review. The seven samples identified were prior to the full roll out of the new profiles. Once identified these were reviewed and additional permissions removed. These roles now map to the updated profiles.	●	●

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

No.	Detailed controls	Relevant exceptions 'if any'	DB	DC
4.3	Member and employer portals adhere to logical security protocols and only relevant information, in accordance with GDPR requirements, is made available.	**Observation** Confirmed by observation of the member and employer portal that security validations were in place and only relevant data was available to view, in accordance with GDPR requirements.* **No exceptions to the company's procedures were noted.**	●	●

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

Trustee signed mandate approval is required for all new bank accounts. Internal authorised signatories are in place for each of the bank accounts, with two signatories necessary to make any changes to the bank mandate.

Administrators creating payments within the administration system do not have access to any of the payment systems, including BACS, internet banking or CHAPs.

A system generated report advises the Finance team of the value of payments to be made that day. This is reconciled to the payment instruction file received prior to payment. The payment systems are configured to require dual authorisation, with an authentication token adding a further layer of security.

Cash forecasting is regularly undertaken. Cash sweeping arrangements are applied, where appropriate, to ensure suitable cash levels are maintained. This process is supported by the routine bank reconciliation ensuring that unreconciled items are fully investigated and accounted for.

No.	Detailed controls	Relevant exceptions 'if any'	DB	DC
4.4	New scheme bank accounts and changes to mandates require two Railpen authorised signatories. Changes to banking providers requires Trustee signed approval.	**Inspection** Confirmed by inspection for a sample of new bank accounts and changes to bank mandates that these were authorised by two existing signatories with appropriate authority levels.* Confirmed by inspection for a sample of changes to banking providers that Trustee signed approval was required.* **No exceptions to the company's procedures were noted.**	●	●

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

No.	Detailed controls	Relevant exceptions 'if any'	DB	DC
4.5	Segregations exist ensuring those initiating benefit payments differ from those processing and authorising the payments.	**Inspection** Confirmed by inspection for a sample of benefit payments, that segregation of duties existed between those initiating, processing and authorising benefit payments.* **No exceptions to the company's procedures were noted.**	●	●
4.6	Access to the BACS application is restricted via unique user sign-in and an authentication card is required to submit payments. A reconciliation is carried out to verify that the BACS submission matches the internal payment processing system.	**Observation** Confirmed by observation of the BACS payments process, that access to the BACS application was restricted via unique user sign-in and an authentication card was required to submit payments.* **Inspection** Confirmed by inspection for a sample of BACS payrolls, that reconciliations had taken place to ensure that the BACS submission matched the internal payment processing system.* **No exceptions to the company's procedures were noted.**	●	●
4.7	Regular bank reconciliations are carried out and reconciling items identified are investigated and action taken where appropriate.	**Inspection** Confirmed by inspection for a sample of dates, that regular bank reconciliations had been undertaken with supporting documentation retained demonstrating that action was taken where appropriate.* **No exceptions to the company's procedures were noted.**	●	●
4.8	Scheme expenses must be approved by an authorised source before payment is made.	**Inspection** Confirmed by inspection for a sample of scheme expenses that they were approved by an authorised source before payment was made.* **No exceptions to the company's procedures were noted.**	●	●

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

No.	Detailed controls	Relevant exceptions 'if any'	DB	DC
4.9	CHAPS payments are subject to approval in line with authorised payment limits by appropriate signatories. Access to the CHAPS payment system is restricted to authorised individuals via unique user sign-in, with segregation between those users able to set up and process payments.	**Observation** Confirmed by observation of the CHAPS payments process that access to the CHAPS application was restricted via unique user sign-in and there was segregation between users able to set up and process payments.* **Inspection** Confirmed by inspection for a sample of CHAPS payments that approval was in accordance with the appropriate signatories list and authorised payment limits.* **No exceptions to the company's procedures were noted.**	●	●

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

5. Managing and monitoring compliance and outsourcing

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

Payroll schedules are maintained within the administration system to ensure that contributions are received in line with payroll cycles and relevant legislation. Employers are advised in advance of data or cash falling due and subsequent reminders are issued once the payment date has passed.

Late contributions are escalated to the scheme sponsor for resolution. The Pensions Regulator is notified, in accordance with requirements, where contributions remain outstanding.

Changes to the contribution rates within the live administration system are only made following appropriate authorisation (including a revised signed schedule of contributions) and testing.

No.	Detailed controls	Relevant exceptions 'if any'	DB	DC
5.1	Receipt of contribution files is monitored against scheme rules and legislative requirements. Where late payment is identified warning letters are issued and employers are reported to The Pensions Regulator in line with breach reporting requirements.	**Inspection** Confirmed by inspection for a sample of events that the Employer Support Breach tracker was maintained and that where late payments were identified, warning letters were issued and breaches were appropriately reported to employers and The Pensions Regulator.* **No exceptions to the company's procedures were noted.**	●	●
5.2	Changes to contribution rates contained within the administration system are appropriately authorised and tested prior to update.	**Inspection** Confirmed by inspection for a sample of contribution rate changes that they had been appropriately authorised prior to update.* **No exceptions to the company's procedures were noted.**	●	●

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

Pension administration activities are governed by service level agreements that are authorised and subject to regular review. Service performance is regularly monitored and assessed against the standards set out in service level agreements.

Expected service levels are detailed in the Service Level Agreements which support the Guide to Service document provided to all employers. The CRMs oversee the full service provision and are the first point of contact for the client, and regularly liaise with the Administration team to discuss service provisions.

Utilising system-produced management information, team managers delegate the incoming work on a daily basis and receive updates from the administrators on work outstanding/in progress. Weekly, senior management meet and consider performance management and resource deployment further.

No.	Detailed controls	Relevant exceptions 'if any'	DB	DC
5.3	The Guide to Services and supporting service level agreement documents outline the scope of services provided. Changes to the Guide to Services and service levels are subject to authorisation. The Guide to Services is reviewed annually by the executive.	**Inspection** Confirmed by inspection of documentation that the Guide to Services was reviewed annually and any changes to the Guide to Services and service levels were authorised.** **No exceptions to the company's procedures were noted.**	●	●
5.4	Performance against service levels is reported to senior management and the executive to consider resource allocation and workload.	**Inspection** Confirmed by inspection for a sample of months, that performance against service levels was reported to and considered by senior management and the executive.** **No exceptions to the company's procedures were noted.**	●	●
5.5	Team managers utilise system-produced management information to allocate casework and review existing workloads on a daily basis, to ensure that service levels can be prioritised.	**Observation** Confirmed by observation that incoming casework and workloads are reviewed daily to ensure appropriate allocation and prioritisation of service levels.** **No exceptions to the company's procedures were noted.**	●	●

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

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

Senior management oversee the complaint and error process and regular reporting is provided and discussed. Root causes are identified and actions put in place to address any issues that arise.

Standard procedures are in place to ensure that complaints are handled effectively and escalated appropriately. A database and schedule are maintained to log the current status of each complaint and record the eventual outcome. Complaints are handled by the relevant administration team, who manage each case through to resolution.

System issues are identified by a review of start of day reporting. These are investigated and resolved.

No.	Detailed controls	Relevant exceptions 'if any'	DB	DC
5.6	Documented procedures are in place to manage complaints. A database and schedule are maintained to monitor the progress of complaints; oversight of this is assigned to particular administrators. Members receive regular progress updates.	**Inspection** Confirmed by inspection that documented procedures were in place to manage complaints.* **Inspection** Confirmed by inspection of the complaints database and schedules that these were maintained to monitor progress of action taken and oversight was assigned to particular administrators.* **Inspection** Confirmed by inspection for a sample of complaints that the member received regular progress updates.* **No exceptions to the company's procedures were noted.**	●	●
5.7	Comprehensive complaints reporting is regularly provided to meetings of senior management and the Trustee for review.	**Inspection** Confirmed by inspection of meeting packs that executive and Trustee meetings were provided with reports detailing the number of types of complaints received along with root cause analysis and action taken.* **No exceptions to the company's procedures were noted.**	●	●

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

No.	Detailed controls	Relevant exceptions 'if any'	DB	DC
5.8	A process is in place to raise and record transaction errors, omissions and issues. Appropriate action is undertaken and regular reporting of events to senior management and the Trustee is in place.	**Observation** Confirmed by observation that a formal process was in place to raise and record identified transaction errors, omissions and issues and to monitor progress of action taken.* **Inspection** Confirmed by inspection for a sample of transaction errors, omissions and issues that appropriate action was undertaken and there was regular reporting to senior management and the Trustee.* **No exceptions to the company's procedures were noted.**	●	●
5.9	System control failures are reported in start of day management reports. These reports are reviewed and failures investigated and resolved.	**Inspection** Confirmed by inspection for a sample of days that application errors had been identified and appropriate action taken to resolve issues identified.* **No exceptions to the company's procedures were noted.**	●	●
5.10	Any loss of investment (LOI) incurred is automatically calculated and invested within the pensions administration system to ensure there is no member detriment. All LOI is allocated to the responsible party and charges are subject to review and authorisation.	**Inspection** Confirmed by inspection for a sample of LOI cases that member records had been updated and charges appropriately allocated and authorised.* Confirmed by inspection that employers were notified of relevant charges.* **No exceptions to the company's procedures were noted.**		●

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

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

Corporate policies are in place to ensure employees are aware of their responsibilities in relation to regulatory reporting. 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, training sessions and through the Benefits Change Board.

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.

Regular training is provided regarding master trust significant and triggering events. Any events raised are assessed by the Master Trust Compliance group for reporting purposes.

No.	Detailed controls	Relevant exceptions 'if any'	DB	DC
5.11	The Technical team monitors regulatory and legislative developments for any potential changes to the pension environment and changes to reporting requirements. Technical updates are provided to technical experts within Member Services and some updates are available to all staff via the intranet. Updates are also presented to the Regulatory Compliance Forum.	**Inspection** Confirmed by inspection of technical update meeting notes and the intranet that regular technical updates were made available.** **Inspection** Confirmed by inspection for a sample of months that regulatory and legislative changes had been considered by the Regulatory Compliance Forum and action taken where required.** **No exceptions to the company's procedures were noted.**	●	●

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

No.	Detailed controls	Relevant exceptions 'if any'	DB	DC
5.12	Routine reporting is undertaken to capture reportable events and enable the Pension Scheme Event Return and HMRC Events Report to be completed and submitted within the required timescales.	**Inspection** Confirmed by inspection of the HMRC Event Report and Pensions Scheme Event Return that items captured by routine reporting were included. Confirmed that these were submitted within required timescales.** **No exceptions to the company's procedures were noted.**	●	●
5.13	Master Trust significant or triggering events are raised with the Master Trust Compliance group who assess and determine reporting requirements to The Pensions Regulator.	**Inspection** Confirmed by inspection that a Master Trust event log was maintained and for a sample of events recorded as reportable, obtained the communications provided to The Pensions Regulator.** **No exceptions to the company's procedures were noted.**		●
5.14	Potential notifiable events are logged for review by the Technical team to determine the reporting requirement to The Pensions Regulator.	**Inspection** Confirmed by inspection that a notifiable events log was maintained by the Technical Team 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.**	●	●

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

6. Reporting to clients

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

Client and member reporting is scheduled via an annual event planner, which is overseen by the Member Services Change and Delivery Committee, to ensure timely preparation and distribution of reports.

Routines within the administration system provide the underlying calculations for Annual Benefit Statements; 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.

Quarterly reports are prepared in accordance with agreed timescales. Each report is fully reviewed and authorised by internal sponsors before submission to the client.

No.	Detailed controls	Relevant exceptions 'if any'	DB	DC
6.1	A formal administration timetable is maintained to ensure the oversight of cyclical events, timely distribution of client reports and benefit statements. This is subject to regular review by the Member Services Continuous Improvement Forum.	**Inspection** Confirmed by inspection for a sample of Member Services Continuous Improvement Forum papers that a formal administration timetable was maintained and subject to regular management oversight to ensure oversight of cyclical events, timely distribution of client reports and benefit statements.* **No exceptions to the company's procedures were noted.**	●	●
6.2	System routines are used to generate cyclical member documentation. Periodic checks are undertaken to ensure accuracy.	**Inspection** Confirmed by inspection for a sample of documents provided to members that periodic checks were undertaken to ensure accuracy.* **No exceptions to the company's procedures were noted.**	●	●
6.3	Quarterly reports are prepared for clients. A circulation of the draft report is provided to internal sponsors before issuance and approval is sought via the report sponsor before publication.	**Inspection** Confirmed by inspection for a sample of client reports that they had been reviewed for accuracy prior to distribution.* **No exceptions to the company's procedures were noted.**	●	●

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

Annual Report and Accounts prepared for pension schemes are complete, accurate and provided within required timescales.

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.

No.	Detailed controls	Relevant exceptions 'if any'	DB	DC
6.4	A timetable for the preparation of the Annual Report and Accounts is established in consultation with scheme auditors.	**Inspection** Confirmed by inspection for a sample of schemes, that a timetable for the preparation of the Annual Report and Accounts was established in consultation with scheme auditors.** **No exceptions to the company's procedures were noted.**	●	●
6.5	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 by inspection for a sample of schemes, that Annual Report and Accounts were prepared in accordance with the latest Statement of Recommended Practice.** Confirmed by inspection for a sample of schemes, that accounts were quality checked prior to issue to the scheme auditor.** **No exceptions to the company's procedures were noted.**	●	●
6.6	Analytical reviews are undertaken periodically throughout the year and investigated as necessary. These are reviewed by a senior accountant.	**Inspection** Confirmed by inspection that analytical reviews were undertaken and the results were reviewed by a senior accountant.** **No exceptions to the company's procedures were noted.**	●	●

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

INFORMATION TECHNOLOGY

7. Restricting access to systems and data

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

Access to Railpen offices is restricted to authorised personnel by an automated access entry system.

The premises operate 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. Where data is held off-site this is maintained by a third party within data centres which are ISO 27001 accredited.

In accordance with our IT Acceptable Use Policy, employees must ensure that visitors are met at reception and adhere to our visitor procedures.

No.	Detailed controls	Relevant exceptions 'if any'
7.1	Access to our premises is restricted to authorised individuals via an automated access system.	**Observation** Confirmed by observation that an automated access entry system is in operation.** **No exceptions to the company's procedures were noted.**
7.2	The premises has 24/7 coverage by security personnel and CCTV operations.	**Enquiry** Confirmed by enquiry with the Facilities Manager that security personnel were on site at all times.** **Observation** Confirmed by observation of the security systems that 24/7 CCTV was in operation.** **No exceptions to the company's procedures were noted.**
7.3	Access to sensitive areas of the business, including critical IT infrastructure, are restricted to authorised personnel only.	**Observation** Confirmed by observation 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.**
7.4	Railpen data held off-premises is managed by organisations that are ISO 27001 accredited.	**Inspection** Confirmed by inspection of the accreditation certificate of the data host and off-site data centre that both were ISO 27001 Information Security Accredited.** **No exceptions to the company's procedures were noted.**

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

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

User Role Profiles are defined by relevant senior management and set up by IT during the employee pre-boarding / onboarding 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 IT team.

End user computing access is secured with a modern biometric multi-factor authentication solution, supported by a robust network domain policy which ensures staff set a minimum complex passphrase of at least 15 characters, and change their password when required. 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 IT and this access is monitored and all IT administrator access is subject to multi-factor authentication.

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. Relevant authentication is required to access the network remotely.

No.	Detailed controls	Relevant exceptions 'if any'
7.5	Enforced network password security protocols are in place requiring users to adopt minimum complex character length and lock out after a number of unsuccessful attempts.	**Inspection** Confirmed by inspection of the network configuration that enforced password requirements were in place.* **No exceptions to the company's procedures were noted.**
7.6	New user access requirements and changes to access are determined and authorised by an appropriate senior officer.	**Inspection** Confirmed by inspection for a sample of new users and changes to roles, 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.**

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

No.	Detailed controls	Relevant exceptions 'if any'
7.7	An IT request is raised by an authorised source when an employee leaves Railpen, instructing IT to deactivate logical access.	**Inspection** Confirmed for a sample of leavers that an IT incident had been raised by an authorised individual to deactivate logical access.* **No exceptions to the company's procedures were noted.**
7.8	Data can be deleted from mobile devices remotely, in the event of theft or loss.	**Inspection** Confirmed by inspection 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.**

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

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

Employer and supplier access to relevant systems can only be approved by authorised individuals within Railpen following appropriate senior authorisation.

Regular access reviews are undertaken with employers and suppliers. Any advised amendments are actioned appropriately.

Employers must attest to comply with data protection requirements prior to accessing data via the employer portal. Data sharing agreements are also in place.

The policy of least privilege is maintained and this extends to masking our data where possible.

No.	Detailed controls	Relevant exceptions 'if any'
7.9	User profiles for client and third party suppliers are created by an authorised Railpen staff member and senior approval is required prior to implementation.	**Inspection** Confirmed by inspection for a sample of client and third party users that access had been created by an authorised Railpen staff member and appropriately authorised prior to implementation.** **Exception** In one out 15 samples taken a third party portal user was created without formal approval of one of the authorised employer contacts. **Management response** Whilst the user was created without approval from an authorised employer contact, the case was reviewed by the relevant Customer Relationship Manager for validity. The importance of reviewing the authorised approver list before granting employer portal access has been reiterated.
7.10	Regular access reviews are issued to clients with portal access to confirm user access remains appropriate.	**Inspection** Confirmed by inspection for a sample of clients with portal access that regular reviews had been issued and access appropriately updated.** **No exceptions to the company's procedures were noted.**

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

No.	Detailed controls	Relevant exceptions 'if any'
7.11	Employers with access to download data through the portal must provide data protection attestations prior to being granted access to data.	**Observation** Confirmed by observation of the employer portal that access to data could only be obtained following confirmation of adherence to GDPR regulations.** **No exceptions to the company's procedures were noted.**
7.12	All testing data is masked where possible to adhere to Railpen's least privileged policy and to safeguard member data.	**Observation** Confirmed by observation that for categories of data that are required to be masked, system enforced controls were in place, in accordance with Railpen's least privileged policy.** Confirmed where decisions had been taken to unmask data, that the decision has been documented and authorised.** **No exceptions to the company's procedures were noted.**

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

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 Service Desk will create an appropriate user ID.

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.

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

No.	Detailed controls	Relevant exceptions 'if any'
7.13	Segregation of incompatible duties is defined within the Access Control Policy, which is referred to as part of the new user set-up process.	**Inspection** Confirmed by inspection of the Access Control Policy that segregation of incompatible duties had been defined.* **No exceptions to the company's procedures were noted.**
7.14	Administrator access to systems is restricted to authorised individuals.	**Inspection or Enquiry** Confirmed by inspection of user profile accounts, that administrator access to systems was restricted to authorised personnel.* **No exceptions to the company's procedures were noted.**
7.15	User profiles are created for each system and role to enforce appropriate segregation of duties.	**Inspection** Confirmed by inspection for a sample of user profile accounts, that permissions and profiles were in line with the access control policy.* **Exception** In seven out of ten BaNCS profiles sampled, the user roles assigned did not map correctly to the documented user role profiles. **Management response** As part of our continual improvement activity new BaNCS role profiles have been introduced and all roles will have been reviewed against these profiles by the end of the July 2026 quarterly review. The seven samples identified were prior to the full roll out of the new profiles. Once identified these were reviewed and additional permissions removed. These roles now map to the updated profiles.
7.16	User access privileges are reviewed by line management on a regular basis.	**Inspection** Confirmed by inspection for a sample of systems that 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.**

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

8. Maintaining integrity of the systems

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

The job scheduler application operates to ensure intraday and overnight IT processes are executed in the correct sequence and at the appropriate time. Where a job fails, this triggers an automatic ticket generation for the IT Service Desk to investigate alongside an Application Support team for externally hosted systems. To support the automated process, the Application Support team performs start of day reviews to provide positive affirmation that the scheduler has run successfully.

For those internally hosted applications which interface with the externally hosted applications, the interfaces are monitored to ensure errors are identified promptly and investigated.

No.	Detailed controls	Relevant exceptions 'if any'
8.1	Start and end of day checks are carried out to ensure data processing is complete, accurate and exceptions identified and investigated.	**Inspection** Confirmed by inspection for a sample of days that health checks had been undertaken. Where issues were identified confirmed that an incident was raised and actioned.* **No exceptions to the company's procedures were noted.**
8.2	Automated batch scheduling is in place. In the event of failure an incident is automatically raised and investigated the following day.	**Inspection** Confirmed through inspection of the incident management system that incidents were created when scheduled events did not occur as planned and that these were investigated the following day and resolved.* **No exceptions to the company's procedures were noted.**
8.3	Transaction failures are reported in start of day management reports. These reports are reviewed and failures are investigated and resolved.	**Inspection** Confirmed by inspection for a sample of days that transaction failures were reported in start of day management reports which were reviewed. Where failures were identified, these were investigated and resolved.* **No exceptions to the company's procedures were noted.**

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

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

All emails use an encryption standard known as Transport Layer Security (TLS) by default, helping to protect information as it travels between organisations. Where sensitive data is being transferred and agreed with the client, Railpen can apply enforced TLS. For large file transfers, Railpen can provide Secure File Transfer Protocol (SFTP), ensuring files are encrypted in transit, with additional file-level password protection applied where required.

We have standard interface files which enable counterparties to send information in a secure, consistent format to enable efficient and accurate upload through our secure employer portal 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.

As an organisation providing services to clients, we recognise the importance of maintaining strong data security standards. We embed data security awareness across the organisation through regular training and supporting policies, including our password and IT security policies. This approach helps strengthen employee awareness and reduce the risk of data loss or compromise.

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.

No.	Detailed controls	Relevant exceptions 'if any'
8.4	SFTP is available for transmitting data to and from external parties.	**Observation** Confirmed by observation that SFTP was available to transmit data files.** **Control not able to be applied.**
8.5	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 by inspection for a sample of external parties participating in auto-encryption, that the necessary configuration had been established to ensure data transmissions were in accordance with the agreed encryption method provided to all employees in the data security policy.** **No exceptions to the company's procedures were noted.**
8.6	Standard interface files are made available to employers to communicate member information. A schedule of expected files is maintained within the system and reminders are issued regarding outstanding and overdue data in accordance with scheme rules and legislation.	**Inspection** Confirmed by inspection that a schedule of expected interface files was maintained within the system and reminders were issued where data is outstanding or overdue in accordance with scheme rules and legislation.** **No exceptions to the company's procedures were noted.**

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

No.	Detailed controls	Relevant exceptions 'if any'
8.7	Incomplete data transmission is identified through end of day checking processes. Where discrepancies are identified employers are contacted to confirm correct changes.	**Inspection** Confirmed by inspection for a sample of days that validation reports had been completed and employers were contacted to investigate any discrepancies.** **No exceptions to the company's procedures were noted.**
8.8	BACS-approved software is used for processing transactions.	**Inspection** Confirmed by inspection of the BACS-approved software suppliers list that software used by Railpen was approved for processing transactions.* **No exceptions to the company's procedures were noted.**
8.9	Data sharing agreements are in place with employers able to access data through the employer portals.	**Inspection** Confirmed by inspection for a sample of employers with portal access that data sharing agreements, were in place.** **Exception** In one out of 10 employers sampled a data sharing agreement was not in place. **Management response** The data sharing agreement will be actioned and the root cause of the exception investigated.

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

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

Our 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 actions arising from the review will be considered and where necessary, implemented by the IT team.

Railpen holds ISO 27001 certification. Our Security Operations Centre (SOC) provides 24/7 coverage, supported by highly skilled and qualified team and an accredited security partner, who have experience of managing complex security incidents. This enables teams to respond quickly to events, minimising disruption to business operations.

No.	Detailed controls	Relevant exceptions 'if any'
8.10	Firewalls are in place to protect the networks from malicious attack.	**Inspection** Confirmed by inspection that firewalls were in operation to protect the networks from malicious attack.** **No exceptions to the company's procedures were noted.**
8.11	IT security reviews are carried out by independent external consultants on a regular basis. Recommended action is undertaken where appropriate.	**Inspection** Confirmed by inspection of the consultant report, that an IT security review had taken place during the year and appropriate follow-up action had taken place.** **No exceptions to the company's procedures were noted.**
8.12	Railpen actively monitors all services on our infrastructure as part of our ongoing security measures. Threat intelligence continuously provided by our SOC enriches and enhances the cyber security maturity of network defences.	**Observation** Confirmed by observation of the SOC dashboard that threats were being actively monitored, contained and escalated to relevant teams where action was required.** **No exceptions to the company's procedures were noted.**

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

Anti-virus definitions are periodically updated across all terminals and servers, deployment and settings are periodically reviewed and updated when required; and patterns of attempted external breaches are monitored.

Railpen 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 IT Acceptable Use Policy and sign a confidentiality agreement upon joining the company. All employees are required to complete on-boarding cyber awareness training along with Security, Continuity and Incident Management mandatory training annually.

Railpen operates a comprehensive Microsoft Defender Extended Detection and Response (XDR) capability that integrates security telemetry from endpoints, email, identities, networks, servers and cloud services to provide centralised monitoring, threat detection and automated response. Threat intelligence and detection definitions are updated automatically to maintain protection against emerging threats.

No.	Detailed controls	Relevant exceptions 'if any'
8.13	Anti-virus software is in operation on all Railpen company infrastructure.	**Inspection** Confirmed by observation of the SOC dashboard that threats were being actively monitored, contained and escalated to relevant teams where action was required.** **No exceptions to the company's procedures were noted.**
8.14	Anti-virus software is deployed and automatically updated by the supplier. IT monitors the application of anti-virus via a management dashboard.	**Observation** Confirmed by observation of the anti-virus dashboard that all Railpen terminals, devices and servers had been updated with the most recent anti-virus settings, rules and patches.** **No exceptions to the company's procedures were noted.**
8.15	Railpen perimeter and internal defences feed into a hybrid managed SOC, where internal and external anomalies are triaged. Trends and patterns are included, where relevant, through the Cyber Security Dashboard for daily monitoring and are included in senior management reporting.	**Inspection** Confirmed by inspection for a sample of senior management reports that patterns of external breaches were monitored and regularly reported.** **Observation** Confirmed by observation that Railpen's perimeter and internal defences feed into a hybrid managed SOC and internal and external anomalies are triaged.** **No exceptions to the company's procedures were noted.**

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

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

Anti-virus protection is delivered through the Extended Detect and Response (XDR) platform. Email filtering technologies scan inbound and outbound communications for malware, spam and malicious content. Suspicious content is quarantined and reviewed before release, with threat signatures automatically updated from the vendor.

Member and employer portals are monitored via web application firewalls which trigger automated alerts to the IT Security Team for action.

No.	Detailed controls	Relevant exceptions 'if any'
8.16	Filters are in place to manage email spam and viruses and automatically block those with malicious links or attachments. Railpen IT can investigate suspicious files in a sandbox environment that is quarantined from the network.	**Inspection** Confirmed by inspection of the network configuration that filters for email spam and viruses were in operation.** **Observation** Confirmed by observation that suspicious files are quarantined from the network and Railpen IT can investigate in a sandbox environment.** **No exceptions to the company's procedures were noted.**
8.17	Email traffic of material size/containing specific criteria is blocked using filtering software. IT will release the email once confirmed as safe.	**Inspection** Confirmed by inspection of the network configuration, that emails of material size or which contain specific criteria were blocked using filtering software.** **Enquiry** Confirmed by enquiry with IT that blocked emails were fully reviewed in their content and attachments before being released.** **No exceptions to the company's procedures were noted.**
8.18	Definitions of threats are continually updated throughout the day by the supplier of the email monitoring system.	**Observation** Confirmed by observation of the email monitoring software that new threat information was being downloaded at regular intervals.** **No exceptions to the company's procedures were noted.**

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

No.	Detailed controls	Relevant exceptions 'if any'
8.19	Interface files received from employers are subject to anti-virus scanning by the data host. Where anomalies are detected, the data host will inform the IT Security team of the incident, including any mitigating actions required.	**Enquiry** Confirmed by enquiry with the IT Security team whether any employer interface files had been blocked by the data host's anti-virus software and action was taken where required.** **Inspection** Confirmed by inspection for a sample of data host monthly security meetings that vulnerabilities and security alerts were discussed.** **No exceptions to the company's procedures were noted.**

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

9. Maintaining and developing systems hardware and software

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

A dedicated Solutions and Delivery function exists to develop and implement changes to the pensions administration system. An annual plan of change is developed based on a number of factors including user feedback, incidents and process improvements.

The plan is agreed by the Benefits Continuous Improvement Forum. The Board approves the strategic change plan and receives updates throughout the year, authorising any changes to the plan.

Change flows through a change lifecycle, from determining the requirements, agreeing the business case, through to development, test and implementation. This is a gated approach ensuring the end user approves the change throughout the change lifecycle to achieve a right first-time approach.

There are a series of test stages, each with distinct environments, with entry and exit criteria which must be authorised by the appropriate Railpen business user before proceeding to the next stage.

Full regression testing is undertaken in advance of major changes and the deployment to live must be authorised by the relevant Railpen business user.

No.	Detailed controls	Relevant exceptions 'if any'
9.1	Change is overseen by the Member Services Leadership Team which comprises of senior departmental representatives. Project prioritisation, status and update reports are provided regularly to the Member Services Leadership Team for oversight and authorisation.	**Inspection** Confirmed by inspection for a sample of reporting to the Member Services Leadership Team that project prioritisation, updates and status reports were provided for consideration and approval.* **No exceptions to the company's procedures were noted.**
9.2	Pension administration systems development is managed through the business change process. Business nominated product owners are responsible for approving the scope at the start of the change process and signing of the testing completion report before the change is approved into the live environment.	**Inspection** Confirmed by inspection for a sample of pension administration systems developments, that a business nominated product owner approved the scope at the start of the change process and signed off the testing completion report before the change was approved into the live environment.* **No exceptions to the company's procedures were noted.**

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

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.

All data migrations require sign-off before the data is transferred into the live environment.

No.	Detailed controls	Relevant exceptions 'if any'
9.3	When data is transferred or modified, validation tests and data cleansing is undertaken to ensure that the data is accurate and complete.	**Inspection** Confirmed by inspection for a sample of data transfers or modifications, that data cleansing and validation tests had been undertaken.** **Control not able to be applied.**
9.4	Data migration or modification requires sign-off before the data is used in the live environment.	**Inspection** Confirmed by inspection for a sample of data migrations or modifications, that there was appropriate sign-off prior to use in the live environment.** **Control not able to be applied.**

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

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

All systems must follow the change management process as defined in the Change Management policy. This includes maintenance, networks, hardware and software. Patching and service updates are carried out on a monthly and quarterly basis to ensure the systems, firmware and supporting infrastructure are patched with the latest security fixes.

Version upgrades of software are planned through the release plan and applied to a lower environment and tested prior to upgrade in the production system.

A patching schedule is maintained. Patches, hardware upgrades and system configurations are all subject to test in a test environment and must be approved prior to being deployed to live.

The Change Advisory Board meets regularly to oversee required changes.

No.	Detailed controls	Relevant exceptions 'if any'
9.5	Systems changes are appropriately tested and authorised prior to being made in a live environment.	**Inspection** Confirmed by inspection for a sample of in-scope system changes, that the change had been tested and authorised prior to going live in line with the Change Management policy.** **No exceptions to the company's procedures were noted.**
9.6	A Change Advisory Board provides oversight and approval of all changes and patches to existing in-scope systems.	**Inspection** Confirmed by inspection for a sample of weekly Change Advisory Board minutes that systems changes and patches were discussed and approved.** **No exceptions to the company's procedures were noted.**
9.7	A patching schedule is maintained and patching is undertaken in test environments before application into live. A process for emergency patching is in place, where necessary.	**Inspection** Confirmed by inspection that a maintenance and patching schedule was maintained and a documented process was in place to cover emergencies. Confirmed for a sample of patches that testing had taken place in the test environment before application into live and correct authorisation was recorded in line with the Change Management process.** **No exceptions to the company's procedures were noted.**

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

No.	Detailed controls	Relevant exceptions 'if any'
9.8	Hardware upgrades are subject to appropriate testing and approval before live implementation, in accordance with the Change Management process.	**Inspection** Confirmed by inspection for a sample of hardware upgrades that they were appropriately tested and approved prior to live implementation, in line with the Change Management process.** **No exceptions to the company's procedures were noted.**

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

10. Recovery from processing interruptions

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

Business Continuity management is provided through 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 unit.
- 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.
- Resilient architecture means we operate from a third party private managed cloud spanning across two Tier 4 data centres located in separate geographic areas, enabling full failover, enabling our staff to continue to work remotely even in the event of a disruption.
- Immutable backup Vault, enabling us to fully recover our systems and data.
- Training and awareness sessions for employees.

Railpen's Business Continuity and Resilience Manager is responsible for overseeing all plans and strategies.

No.	Detailed controls	Relevant exceptions 'if any'
10.1	Disaster recovery plans are in place for each business function outlining business critical areas which are subject to regular review and are signed-off by Senior Management.	**Inspection** Confirmed by inspection for a sample of different functions that disaster recovery plans were in place and were subject to regular review and were signed off by Senior Management.* **No exceptions to the company's procedures were noted.**
10.2	Disaster recovery plans are subject to regular testing to ensure the plans remain relevant and the business is prepared to respond to a range of potential events.	**Inspection** Confirmed by inspection for a sample of functions that the disaster recovery plan was subject to regular testing.* **No exceptions to the company's procedures were noted.**

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

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

All production and critical servers are backed up daily and are stored for 31 days within Railpen. Hosting supplier backups are retained for 13 months, which include the core pension administration system. Additionally, all critical servers are replicated to the Disaster Recovery Data Centre. Data replication takes place as data is written/changed. We routinely test all servers for recoverability. Ransomware data protection service is also deployed and managed by Railpen's critical service provider.

No.	Detailed controls	Relevant exceptions 'if any'
10.3	A Railpen backup policy is in place that identifies requirements for the scope, schedule, retention period and location of backups.	**Inspection** Confirmed by inspection that a backup policy was in place and that the scope, schedule, retention period and location of backups requirements had been identified.* **No exceptions to the company's procedures were noted.**
10.4	Regular restores of information are performed to verify the reliability, accuracy and integrity of the restore process.	**Inspection** Confirmed by inspection for a sample of data restores that files had been successfully recovered. Where discrepancies were identified, confirmed that these were investigated and resolved.* **No exceptions to the company's procedures were noted.**

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

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

We have a dedicated Service Desk team within 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. Service levels are in place for response and resolution times and are regularly monitored.

A dedicated Incident Support Manager is in place. Incidents relating to the pensions administration platform and its usage are reviewed on a fortnightly basis to determine root cause. Additional training, process revisions or system fixes may be instigated. In addition, a Member Services Operating Committee meets monthly to review incident trends and analysis.

A major incident management process is in place to manage and resolve larger scale incidents. Where major incidents occur the root cause is identified, this investigation includes incidents involving external hosts who are required to provide their own root cause reporting to Railpen. Actions required to eliminate future incidents are tracked internally or with the supplier until they are resolved.

No.	Detailed controls	Relevant exceptions 'if any'
10.5	A Service Desk system is used to log IT issues reported. IT prioritises issues and Service Level Agreements (SLAs) are in place for timely resolution.	**Inspection** Confirmed by inspection for a sample of issues logged on the Service Desk, that a priority status was assigned and a record was maintained which noted the date of resolution.* **Exception** In one out of 25 samples, the ticket had breached the SLA and not been closed. **Management response** Investigation noted that the ticket in question had been actioned and resolved but not formally closed. The root cause was human error, and agents have been reminded to formally close all tickets on resolution.
10.6	A Major Incident Management policy is in place to establish and enforce a process to resolve major incidents across all Railpen technology environments within agreed timescales. The external host is required to provide a major incident report within three days of the incident happening. Actions are tracked with the supplier.	**Inspection** Confirmed by inspection that a Major Incident Management policy is in place to establish and enforce a process to resolve major incidents across all Railpen technology environments within agreed timescales.* **Inspection** Confirmed by inspection for a sample of major incidents that a report was provided by the external host within three days of the incident occurring, and the actions were tracked with the supplier.* **No exceptions to the company's procedures were noted.**

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

No.	Detailed controls	Relevant exceptions 'if any'
10.7	A problem management process is in place that defines those IT incidents that require additional investigation. Tools are in place to review the root cause and identify system and people rectification plans to reduce and/or eliminate the incidents reoccurring.	**Inspection** Confirmed by inspection that a problem management process is in place and that it defines IT incidents that require additional investigation.* Confirmed by inspection for a sample of problem IT incidents that trend analysis had been completed and regular reports had been issued to stakeholders identifying system and people rectification plans to reduce and/or eliminate the incident from reoccurring.* **No exceptions to the company's procedures were noted.**

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

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

System capacity is monitored in terms of volume and performance. Our data hosts notify us of any issues along with any remedial action that has been taken.

The Application Support team monitors the performance of the applications on a daily basis, looking at key metrics such as computer processing unit usage. The internal Web team monitors the performance of employer and member portals. Both teams investigate and rectify any issues identified.

Planned changes which are deemed to materially impact the system are considered in terms of the non-functional requirements including performance and security.

No.	Detailed controls	Relevant exceptions 'if any'
10.8	Capacity and performance monitoring is undertaken by our data host. Notifications are issued advising of action taken to maintain prescribed limits.	**Inspection** Confirmed by inspection for a sample of monthly data host service review reports that performance metrics were discussed and actions raised to maintain prescribed limits.* **No exceptions to the company's procedures were noted.**
10.9	A non-functional impact assessment is undertaken for any release into live. Where applicable, performance testing is carried out in a pre-production environment to minimise degradation following a change.	**Inspection** Confirmed by inspection for a sample of systems developments and implementation, that an impact assessment had been undertaken before live implementation. Where applicable, performance testing was carried out in a pre-production environment.* **No exceptions to the company's procedures were noted.**
10.10	Performance monitoring of the member portals is carried out by the internal Web team who will be alerted to any issues relating to system performance, including downtime and security issues. All problems are investigated and rectified.	**Observation** Confirmed by observation of the member portals that performance monitoring was carried out by the internal Web team and they are alerted of any issues relating to system performance, including downtime and security issues.* **No exceptions to the company's procedures were noted.**
10.11	The Application Support team undertakes daily health checks and review the incidents to identify potential areas for performance improvement.	**Inspection** Confirmed by inspection for a sample of days that health check had been undertaken. Where issues were identified confirmed that an incident was raised and actioned.* **No exceptions to the company's procedures were noted.**

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

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 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 off-site data centre which guarantees hardware availability; this also benefits from redundant capacity components; dual powered equipment; and is ISO 27001 accredited.

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.

No.	Detailed controls	Relevant exceptions 'if any'
10.12	IT infrastructure rooms are protected against fire, power failure, and unauthorised access.	**Observation** Confirmed by observation that environmental controls were in operation to protect infrastructure rooms from fire, power failure and unauthorised access.** **No exceptions to the company's procedures were noted.**
10.13	An IT asset register is in place and maintained to record key devices held by staff.	**Inspection** Confirmed by inspection for a sample of assets that they had been correctly recorded in the IT asset register.* **Exception** In two out of 25 assets sampled, the asset was not held by the specific staff member as recorded in the register. **Management response** In each of the two cases, the asset had been returned to Railpen by the staff member. However, a procedure step was missed, resulting in the register entry not being updated. The register has now been corrected and has been reviewed to ensure where assets have been returned these entries are correct. Additional validation checks will be performed on the register to ensure its accuracy and completeness.
10.14	Laptops and portable devices are password protected and have mandatory password requirements.	**Observation** Confirmed by observation of the network settings that enforced password requirements were in place for all laptops and portable devices.* **No exceptions to the company's procedures were noted.**

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

11. Managing and monitoring compliance and outsourcing

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

Oversight of the data host is managed on a day-to-day basis by IT. A signed contract and service definition document is in place. This outlines the roles and responsibilities of Railpen and the data hosts and includes Key Performance Indicators (KPIs) and SLAs which are subject to regular review.

Our contracts are reviewed in line with our Supplier Oversight Policy.

No.	Detailed controls	Relevant exceptions 'if any'
11.1	Authorised contracts are in place with critical hardware and software providers. These detail support services and SLAs.	**Inspection** Confirmed by inspection for a sample of contracts with critical hardware and software providers that they detailed support agreements and SLAs.** **No exceptions to the company's procedures were noted.**
11.2	The Supplier Oversight Policy outlines those circumstances in which contract reviews take place. Reviews are led by the relationship manager to confirm ongoing compliance.	**Inspection** Confirmed by inspection for a sample of contract reviews, identified in accordance with the Supplier Oversight Policy, that they had taken place and actions and matters arising had been recorded and tracked.** **No exceptions to the company's procedures were noted.**

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

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

IT Service Management hold monthly service review meetings with the data host where SLAs and KPIs are discussed. Monthly reporting packs are discussed as part of these relationship meetings. The reporting includes analysis of the service provision and performance responses for the period.

No.	Detailed controls	Relevant exceptions 'if any'
11.3	IT Services provided by Subservice Organisations are subject to regular monitoring and review in accordance with the Supplier Oversight Policy and process.	**Inspection** Confirmed by inspection that for Subservice Organisations providing IT services, supplier monitoring was carried out in line with the Supplier Oversight Policy.** **No exceptions to the company's procedures were noted.**
11.4	Relationship managers are assigned for each Subservice Organisation engaged by Railpen. They are responsible for ensuring the service is monitored and is compliant with SLAs.	**Inspection** Confirmed by inspection for a sample of Subservice Organisations that a relationship manager was assigned, regular service reports were received and any deviation from SLAs was challenged and investigated by the relationship manager.** **No exceptions to the company's procedures were noted.**

** Underlying test performed by the Service Auditors.*
*** Underlying test performed by Railpen Internal Audit team, subsequently reviewed by the Service Auditors.*

REPORT OF THE SERVICE AUDITOR

Independent Service Auditor's assurance report on control activities at Railpen Limited (the 'Service Organisation')

Scope

We have been engaged to report on Railpen Limited's description of its pensions administration services and related information technology for clients throughout the year ended 31 December 2025 found on pages 15-76 (the 'description'), and on the suitability of the design and operating effectiveness of control activities to achieve the related control objectives.

Railpen Limited uses an Information Technology Service Organisation (the 'Subservice Organisation') for its systems development, data hosting and backups. The description includes only the control activities and related control objectives of Railpen Limited and excludes the control objectives and related control activities of the Subservice Organisation. Our examination did not extend to control activities of the Subservice Organisation.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls contemplated in the design of the Railpen Limited's control activities are suitably designed and operating effectively, along with related control activities at Railpen Limited. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

While the control activities and related control objectives may be informed by Railpen Limited's need to satisfy legal or regulatory requirements, our scope of work and our conclusions do not constitute assurance over compliance with those laws and regulations.

Service organisation's responsibilities

Railpen Limited is responsible for: preparing the description and the accompanying Report by the Directors set out on pages 4 and 5, including the completeness, accuracy, and method of presentation of the description and the Report by the Directors; providing the pension administration and related information technology 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 control activities to achieve the stated control objectives.

The control objectives stated in the description include the internal control objectives developed for pension administration and related information technology services as set out in the ICAEW Technical Release AAF 01/20.

Our independence and quality control

In carrying out our work, we have complied with the Institute of Chartered Accountants in England and Wales (ICAEW) Code of Ethics, which includes independence and other requirements founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour. The firm applies International Standard on Quality Control (UK) 1 and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Service Auditor's responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the control activities to achieve the related control objectives stated in that description based on our procedures. We conducted our engagement in accordance with International Standard on Assurance Engagements 3000 (Revised), International Standards on Assurance Engagements 3402 and ICAEW Technical Release AAF 01/20. Those standards and guidance require that we comply with ethical requirements and plan and perform our procedures to obtain reasonable

assurance about whether, in all material respects, the description is fairly presented and the control activities were suitably designed and operating effectively to achieve the related control objectives stated in the description.

Our work involved performing procedures to obtain evidence about the presentation of the description and the suitability of design of control activities and operating effectiveness of those controls. Our procedures included assessing the risks that the description is not fairly presented and that the control activities were not suitably designed or operating effectively to achieve the related control objectives stated in the description. Our procedures also included testing the operating effectiveness of those control activities that we consider necessary to provide reasonable assurance that the related control objectives stated in the description were achieved. Our procedures also include evaluating the overall presentation of the description, the suitability of the control objectives stated therein, and the suitability of the criteria specified by Railpen Limited and described on pages 15-16.

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

Inherent limitations

Railpen Limited's description is prepared to meet the common needs of a broad range of clients and their auditors and may not, therefore, include every aspect of Railpen Limited's activities that each individual client may consider important in its own particular environment. Also, because of their nature, control activities at Railpen Limited 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 suitability of the design or operating effectiveness of the control activities would be inappropriate.

Opinion

In our opinion, in all material respects, based on the criteria described in Railpen Limited's specified control objectives in the Directors' assertion on pages 4 and 5.

a) the description on pages 15-76 fairly presents Railpen Limited's pensions administration and related information technology services as designed and implemented throughout the year ended 31 December 2025;

b) the control activities related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described control activities operated effectively throughout the year ended 31 December 2025; and

c) the control activities tested, were operating with sufficient effectiveness to provide reasonable assurance that the control objectives stated in the description were achieved throughout the year ended 31 December 2025.

Description of tests of control activities

The specific control activities tested and the nature, timing and results of those tests are detailed on pages 19-76.

Use of report

This report and the descriptions of tests of control activities and results thereof are made solely for the use of the directors, as a body, of Railpen Limited, and solely for the purpose of reporting on the control activities of Railpen Limited in accordance with the terms of our engagement letter dated 16 February 2026.

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, including the descriptions of tests of control activities and results thereof to Railpen Limited and clients using Railpen Limited's pensions administration services (clients), and to the auditors of Railpen Limited and such clients to enable Railpen Limited, clients and their auditors to verify that a Service Auditor's Report has been commissioned by the Directors of Railpen Limited and issued in connection with the control activities of Railpen Limited 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 Railpen Limited for our work, for this report or for the opinions we have formed.

Assure UK
London

22 July 2026

Assure UK
107 Cheapside
London
EC2V 6DN

T 020 7112 8300
E info@assureuk.co.uk
W www.assureuk.co.uk

PRIVATE AND CONFIDENTIAL

The Board of Directors Railpen Limited
100 Liverpool Street
London
EC2M 2AT

16 February 2026
Our ref:GB/BP/OB

Dear Sirs

Engagement letter – ISAE 3402 / AAF 01/20 Type 2 Service Auditors' Assurance Report for RPS schemes

Thank you for appointing Assure (UK) Limited as assurance Service Auditors. 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 the Board of Directors of Railpen 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 Railpen Limited ("**Assurance Report**").

The AAF 01/20 Assurance Report will review the control activities in place in the Service Organisation and the suitability and effectiveness of these control activities for Railpen RPS operations for the year ending 31 December 2025 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 01/20 "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 01/20**").

Further details regarding the Assurance Report AAF 01/20 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 ("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 may 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 2 to be included on your website and on the basis, that our report can only be viewed to these website visitors who confirm they have read and agree the wording set out in appendix 2.

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 your liability under this Agreement to £1,000,000 and clause 19.3 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.

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 Gareth Burton on 020 7112 8300.

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.

Nic Cromack

Signature of authorised person on behalf of the Railpen Limited

Print name: Nic Cromack

Date: 27 February 2026

Assure UK
Chartered Accountants and Registered Auditor

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.

1.3. Defined terms set out in our Engagement Letter shall be read and construed in the same way within these Terms of Business unless otherwise stated.

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 01/20 (**"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 activities 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.

2.7. Our duty of care is to you and no one else unless we expressly agree in writing otherwise you agree that the work carried out or contemplated in accordance with this Agreement is provided to you solely by Assure UK and your relationship is with Assure UK and not with any director, employee consultant or otherwise, who will therefore assume, to the maximum extent permitted by law, no personal liability to you.

3. Your responsibilities

3.1. The Directors are responsible for the design, implementation and operation of control activities 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 activities 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 01/20 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 activities

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. The Assurance Report will be issued for the purpose of reporting on the Service Organisation's controls, in accordance with this Agreement.

5.2. We do not accept any responsibility or liability to any third party including, but not limited to, the Service Organisation's existing and prospective clients, and those clients' professional advisors (such as their auditors), unless otherwise agreed by us in writing.

5.3. Subject to the conditions set out in this clause 5, we permit the disclosure of the Assurance Report, whether in electronic format or otherwise, to any third party provided that there is no change to the wording, form, content or presentation of the Assurance Report and that it is disclosed as a complete document. In particular, disclosure of the Assurance Report must be made with the Disclaimer Letter published in the appendix to the Assurance Report and with the inclusion of the prominent written statement at the front of the Assurance Report. The wording of this Disclaimer Letter will be agreed between us and failing such agreement any such disclosure may not be permitted.

5.4. The third parties referred to in clause 5.3 may include, but are not limited to, the Service Organisation's existing and prospective clients, and those clients' professional advisors (such as their auditors). We also acknowledge that the Service Organisation may choose to make the Assurance Report publicly available, which may include publishing the Assurance Report on the internet.

5.5. While we acknowledge that the Service Organisation may make the Assurance Report publicly available on the internet, if the Service Organisation explicitly

sends the Assurance Report to its bankers or its professional indemnity insurers, it will first seek written agreement to certain terms (to be agreed between us if the situation arises). These terms will confirm the purpose of the Assurance Report and acknowledge that we have no responsibility or liability to the Service Organisation's bankers or its professional indemnity insurers.

5.6. We reserve the right to request amendments to the electronic version of the Assurance Report available on the internet if we are not satisfied with the wording or the manner in which it is presented. If requested, the Service Organisation will make such reasonable amendments as are agreed between us, and will use reasonable endeavours to ensure that the previous wording is no longer available on the internet or otherwise disclosed to third parties.

5.7. 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 duties as auditor belong solely to us 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 (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, 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 these conditions 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 condition 7.2 and condition 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. Your 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.

Assure UK
Chartered Accountants and Registered Auditor

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. Notwithstanding clause 7.1 and 7.4, we accept responsibility and shall be liable to and indemnify Railpen for any and all losses directly suffered by Railpen to the extent that such loss arises as a result of the negligence, wilful default, fraud, or breach of applicable law.

7.6. 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.

7.7. 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).

7.8. 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. These terms of business and the engagement letter (together the "Agreement") constitute 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. 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. 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. The Agreement is between you and Assure UK. Notwithstanding the fact that certain Services under

the Agreement may be carried out by personnel provided to Assure UK through subcontracting agreements, to the extent permissible by law you agree that none of the subcontractors will have any liability to you and you will not bring any claim or proceedings of any nature (whether in contract, tort, breach of statutory duty or otherwise and including but not limited to, a claim for negligence) in any way in respect of or in connection with this Agreement against any subcontractors that we may use to provide the Services. The Agreement is between you and Assure UK and Assure UK will be responsible for any losses to Railpen Limited as a result of the actions of subcontractors provided by Assure UK. The foregoing exclusion does not apply to any liability, claim or proceeding founded on an allegation of fraud or other liability that cannot be excluded under English Law.

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. Neither of us may assign or otherwise transfer the benefit of this Agreement without the other's prior written consent. Further, neither of us will directly nor indirectly agree to assign or transfer any claim against the other arising out of this Agreement to any other person.

10.4. *Third party rights* - No person who is not a party to the Agreement other than our subcontractors if any, 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 with reasonable care and skill. We will endeavour to notify the Directors/Management as soon as reasonably practicable if we become aware of any conflict of interest to which we become subject.

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 as Directors 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 the Directors 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, HMRC 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 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, HMRC or other government or regulatory authority.

11.5. The working papers prepared in conjunction with our assurance report 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 partner in or employee of our firm from taking such steps as

Assure UK
Chartered Accountants and Registered Auditor

are necessary to comply with professional or ethical rules of any relevant professional body of which a partner in or employee of our firm 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).

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. Provision of services regulations 2009

12.1. In accordance with the disclosure requirements of the Provision of Services Regulations 2009, our professional indemnity insurer is Howden Insurance Brokers Limited, 10th Floor, 5 Churchill Place, London, E14 5HU. The territorial coverage is worldwide excluding professional business carried out from an office in the United States of America or Canada and excludes any action for a claim bought in any court in the United States of America or Canada.

12.2. Details of our audit registration can be viewed at www.auditregister.org.uk for the UK under reference number C003443000. We confirm that we are Statutory Auditors eligible to conduct audits under the Companies Act 2006, and eligible to undertake Service Auditor services.

13. Intellectual property

13.1. 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.

13.2. Our Assurance Report is ©Assure (UK) Limited and we retain all copyrights and other intellectual property rights in relation to the Assurance Report.

13.3. We own all intellectual property rights in our name and logo. You are not permitted to use our name and logo without our prior written consent.

14. Electronic communications

14.1. 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.

14.2. 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.

15. Fees and expenses

15.1. Our fees are based upon the degree of responsibility and skill involved, the importance and value of the advice that we provide, the level of risk, and the time necessarily occupied on the work.

15.2. If we provide you with an estimate of our fees for any specific work, then the estimate will not be contractually binding unless we explicitly state that this will be the case. Unless otherwise agreed to the contrary our fees do not include the costs of any third party, counsel or other professional fees.

15.3. Where requested we may indicate a fixed fee for the provision of specific services or an indicative range of fees for a particular assignment. If it becomes apparent to us, due to unforeseen circumstances, that a fee quote is inadequate, we reserve the right to notify you of a revised figure or range and to seek your agreement thereto.

15.4. Fees are charged separately for each of the main classes of work we perform for you and will be billed at appropriate intervals during the course of the year. Our fees are exclusive of VAT which will be added where it is chargeable. Unless agreed otherwise in writing, any disbursements we incur on your behalf and expenses incurred in the course of carrying out our work for you will be added to our invoices where appropriate.

15.5. Fees are due for payment within 30 days of presentation of our invoice or as agreed.

15.6. All queries on fee accounts rendered by us must be raised in writing within 7 days of the account being received. Any account received by you and not queried in writing within 7 days of receipt will be deemed to be accepted as a reasonable charge for the work done.

15.7. We reserve the right to charge interest on overdue accounts at the current rate under the late Payment of Commercial Debts (Interest) Act 1998. We also reserve the right to terminate our engagement and cease acting for you on giving written notice if payment of any fees billed is unduly delayed. We intend to exercise these rights only where it is fair and reasonable to do so.

15.8. If a client company, LLP, trust, or other entity is unable or unwilling to settle our fees we reserve the right to seek payment from the individual (or parent entity) giving us instructions on behalf of the client and we shall be entitled to enforce any sums due against the group, entity or individual nominated to act for you.

15.9. Insofar as we are permitted to do so by law or professional guidelines, we reserve the right to exercise a lien over all funds, documents and records in our possession, relating to all engagements for you until all outstanding fees and disbursements are paid in full.

15.10. In some circumstances commissions or other benefits may become payable to us, in respect of introductions to other professionals or transactions which we arrange for you. If this happens, you will be notified in writing of the amount, the terms of payment and receipt of any such commissions or benefits.

15.11. If it becomes necessary for us to liaise with, or make a report to a regulator or public sector body, as a result of any statutory duty imposed upon us by legislation or other regulation, including after our engagement has ended, we reserve the right to charge for work undertaken in accordance with these reporting duties.

15.12. If, for any reason it becomes necessary for us to withdraw from the engagement, our fees for work performed up to that date will be payable by you.

16. Data protection

16.1. Both parties will adhere to and comply in all respects with all applicable requirements of the Data Protection Legislation. This clause 16 is in addition to, and does not relieve, remove or replace, a party's obligations under the Data Protection Legislation (being the UK Data Protection Legislation and (for so long as and to the extent that the law of the European Union has legal effect in the UK) the GDPR (General Data Protection Regulations) and any other directly applicable European Union regulation relating to privacy).

16.2. In this clause 16, the following definitions shall apply:

Assure UK
Chartered Accountants and Registered Auditor

'**client personal data**' means any personal data provided to us by you, or on your behalf, for the purpose of providing our services to you, pursuant to our engagement letter with you;

'**data protection legislation**' means all applicable privacy and data protection legislation and regulations in force from time to time in the UK including, but not limited to the GDPR (as it forms part of domestic law by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the "UK GDPR")), the Data Protection Act 2018 and any applicable national laws, regulations and secondary legislation in the UK relating to the processing of personal data and the privacy of electronic communications, as amended, replaced or updated from time to time;

'**controller**', '**data subject**', '**personal data**', and '**process**' shall have the meanings given to them in the data protection legislation;

'**GDPR**' means the General Data Protection Regulation ((EU) 2016/679).

16.3. We shall each be considered an independent data controller in relation to the client personal data. Each of us will comply with all requirements and obligations applicable to us under the data protection legislation in respect of the client personal data.

16.4. You shall only disclose client personal data to us where:

(i) you have provided the necessary information to the relevant data subjects regarding its use (and you may use or refer to our privacy notice available at https://assureuk.sharefile.com/share/view/s51f6409b84f4753b);

(ii) you have a lawful basis upon which to do so, which, in the absence of any other lawful basis, shall be with the relevant data subject's consent; and

(iii) you have complied with the necessary requirements under the data protection legislation to enable you to do so.

16.5. We shall only process the client personal data:

(i) in order to provide our services to you and perform any other obligations in accordance with our engagement with you;

(ii) in order to comply with our legal or regulatory obligations; and

(iii) where it is necessary for the purposes of our legitimate interests and those interests are not overridden by the data subjects' own privacy rights. Our privacy notice (available at https://assureuk.sharefile.com/share/view/s51f6409b84f4753b) contains further details as to how we may process client personal data.

16.6. For the purpose of providing our services to you, pursuant to our engagement letter, we may disclose the client personal data to our regulatory bodies or other third parties (for example, our professional advisors or service providers). The third parties to whom we disclose such personal data may be located outside of the European Economic Area (EEA). We will only disclose client personal data to a third party outside of the EEA with your written consent. If such consent is provided, then we shall ensure that the transfer is undertaken in compliance with data protection legislation and appropriate safeguards are put in place.

16.7. We shall maintain commercially reasonable and appropriate security measures, including administrative, physical and technical safeguards, to protect against unauthorised or unlawful processing of the client personal data and against accidental loss or destruction of, or damage to, the client personal data.

16.8. In respect of the client personal data, provided that we are legally permitted to do so, we shall promptly notify you in the event that:

a) we receive a request, complaint or any adverse correspondence from or on behalf of a relevant data subject, to exercise their data subject rights under the data protection legislation or in respect of our processing of their personal data;

b) we are served with an information, enforcement

or assessment notice (or any similar notices), or receive any other material communication in respect of our processing of the client personal data from a supervisory authority as defined in the data protection legislation (for example in the UK, the Information Commissioner's Officer); or

c) we reasonably believe that there has been any incident which resulted in the accidental or unauthorised access to, or destruction, loss, unauthorised disclosure or alteration of, the client personal data.

16.9. Upon the reasonable request of the other, we shall each co-operate with the other and take such reasonable commercial steps or provide such information as is necessary to enable each of us to comply with the data protection legislation in respect of the services provided to you in accordance with our engagement letter with you in relation to those services.

17. Quality of service

17.1. Our objective is to provide you with a high quality 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 Client Service Partner responsible for providing the Services to you. If you would prefer to discuss the matter with someone other than your Client Service Partner, or you wish to make a complaint please call or write to Lorraine Hawkins Assure UK's nominated Complaints Officer.

17.2. 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 Conduct Department, Metropolitan House, 321 Avebury Boulevard, Milton Keynes MK9 2FZ

18. Invalidity

18.1. 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.

19. Applicable law

19.1. 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.

19.2. 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.

19.3. 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.

19.4. No party shall be liable to the other if it fails or is delayed in meeting its obligations under this Agreement because of matters beyond its reasonable control including but not limited to, (a) an act of God, fire, flood, drought, earthquake, windstorm, or other natural disaster; (b) an act of war, terrorism, civil war, riots, or armed conflict, (c) radioactive, nuclear, chemical or biological contamination or sonic boom, (d) any law, or action taken by a governmental order, (e) interruption or failure of utility or internet services.

19.5. 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.

20. Data retention

20.1. We will only retain your personal data for as long as is necessary to fulfil the purposes for which it is collected.

20.2. When assessing what retention period is appropriate for your personal data, we take into consideration:

- the requirements of our business and the services provided;
- any statutory or legal obligations;
- the purposes for which we originally collected the personal data;
- the lawful grounds on which we based our processing;
- the types of personal data we have collected;
- the amount and categories of your personal data; and
- whether the purpose of the processing could reasonably be fulfilled by other means.

20.3. We will permanently destroy or return all Personal Data after the end of the provision of services relating to the Processing of such Personal Data subject to our data retention policy outlined below. We will adopt proper destruction methods that are widely recognised in the industry as sufficiently rendering retrieval, restoration, or reconstruction of any Personal Data practicably impossible, regardless of the form or media.

All the audit files and working papers produced by this firm follow our audit system. They are retained for the later of 6 years from the balance sheet date or 5 years from the date of the audit report.

21. Restrictive Covenants

21.1. Neither Party shall, directly or indirectly, solicit the employment of any of the other's directors or employees, as the case may be, involved in provision or performance of the services while the services are being performed or for a period of 12 months following their completion or following termination of this Agreement (howsoever terminated), without the prior written consent of the other. This prohibition shall not prevent either party at any time from running recruitment advertising campaigns nor from offering employment to any of the directors or employees, as the case may be, of the other party who may respond to such campaigns provided that they have not been solicited in breach of this clause.