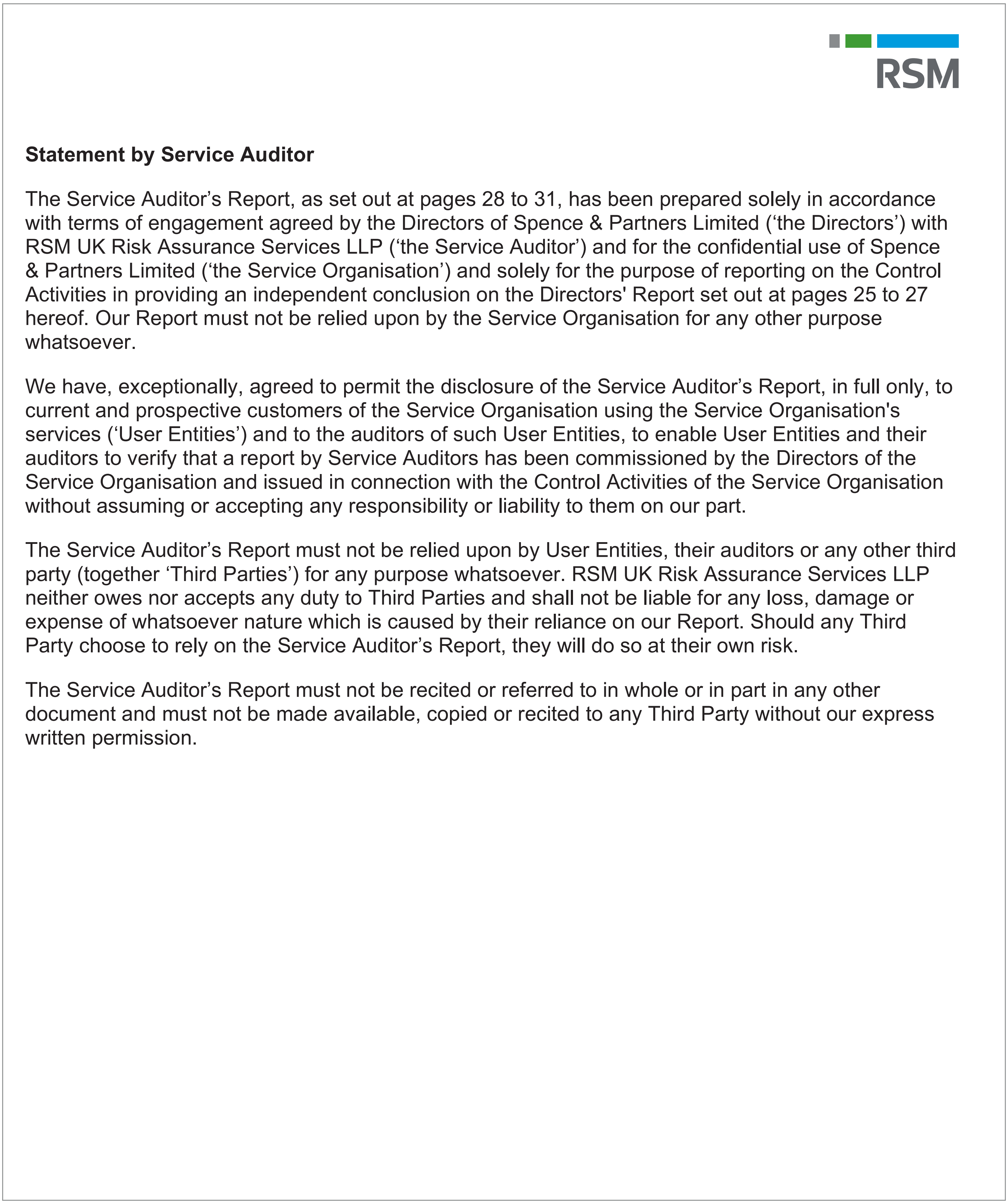
SPENCE

Assurance Report on Internal Controls (AAF 01/20 and ISAE 3402)

AN EFFICIENT AND COMPREHENSIVE SERVICE TO PENSION SCHEMES

For the period 1 January 2022 to 31 December 2022

Statement of Reporting Accountants



Statement by Service Auditor

The Service Auditor’s Report, as set out at pages 28 to 31, has been prepared solely in accordance with terms of engagement agreed by the Directors of Spence & Partners Limited (‘the Directors’) with RSM UK Risk Assurance Services LLP (‘the Service Auditor’) and for the confidential use of Spence & Partners Limited (‘the Service Organisation’) and solely for the purpose of reporting on the Control Activities in providing an independent conclusion on the Directors' Report set out at pages 25 to 27 hereof. Our Report must not be relied upon by the Service Organisation for any other purpose whatsoever.

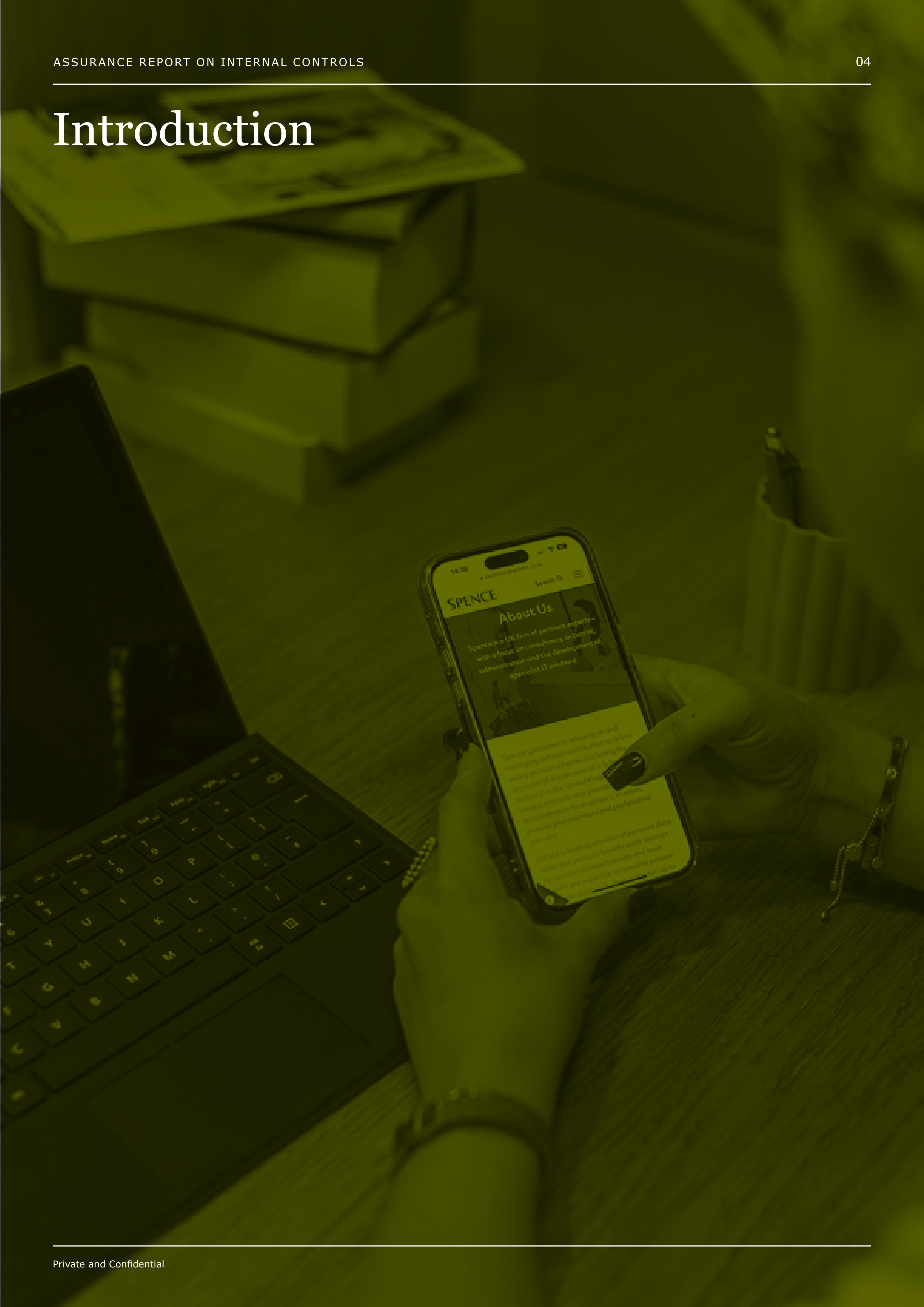
We have, exceptionally, agreed to permit the disclosure of the Service Auditor’s Report, in full only, to current and prospective customers of the Service Organisation using the Service Organisation's services (‘User Entities’) and to the auditors of such User Entities, to enable User Entities and their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

The Service Auditor’s Report must not be relied upon by User Entities, their auditors or any other third party (together ‘Third Parties’) for any purpose whatsoever. RSM UK Risk Assurance Services LLP neither owes nor accepts any duty to Third Parties and shall not be liable for any loss, damage or expense of whatsoever nature which is caused by their reliance on our Report. Should any Third Party choose to rely on the Service Auditor’s Report, they will do so at their own risk.

The Service Auditor’s Report must not be recited or referred to in whole or in part in any other document and must not be made available, copied or recited to any Third Party without our express written permission.

What’s inside

Introduction



Introduction

The Directors of Spence & Partners Limited (“Spence”) are pleased to present our report detailing the control procedures that are in place relating to Spence’s business operations in providing pension administration and pension database services.

This report covers the year ended 31 December 2022 and has been prepared in accordance with the Technical Release AAF 01/20 “Assurance Reports on Internal Controls of Service Organisations made available to Third Parties” published by the Institute of Chartered Accountants in England and Wales (“the ICAEW”).

The International Standard on Assurance Engagements (“ISAE”) 3402, Assurance Reports on Controls at a Service Organisation, was issued in December 2009 by the International Auditing and Assurance Standards Board (“IAASB”), which is part of the International Federation of Accountants (“IFAC”). The ISAE 3402 provides an international assurance standard to allow public accountants to issue a report on the controls of a service organisation that are likely to impact, or be a part of, a user organisation’s system of internal controls over financial reporting.

As the control objectives are consistent with ISAE 3402, Spence will be reporting on both standards for this reporting period.

The control objectives are set out on pages 32 to 35 and we demonstrate how we meet these on pages 36 to 62. These measures have been audited and reported upon by RSM UK Risk Assurance Services LLP. This is the eleventh such report we have published.

Spence provides a full range of pension administration services and is a leading provider of pension data audit and pension benefit audit services for pension scheme trustees. We see database work as core to our business and the strength of our pension database expertise has enabled us to develop a powerful suite of software to perform remedial pension scheme data work. Such work is often required where a scheme is considering buying out its liabilities, or during Pension Protection Fund (“PPF”) or Financial Assistance Scheme (“FAS”) assessment periods.

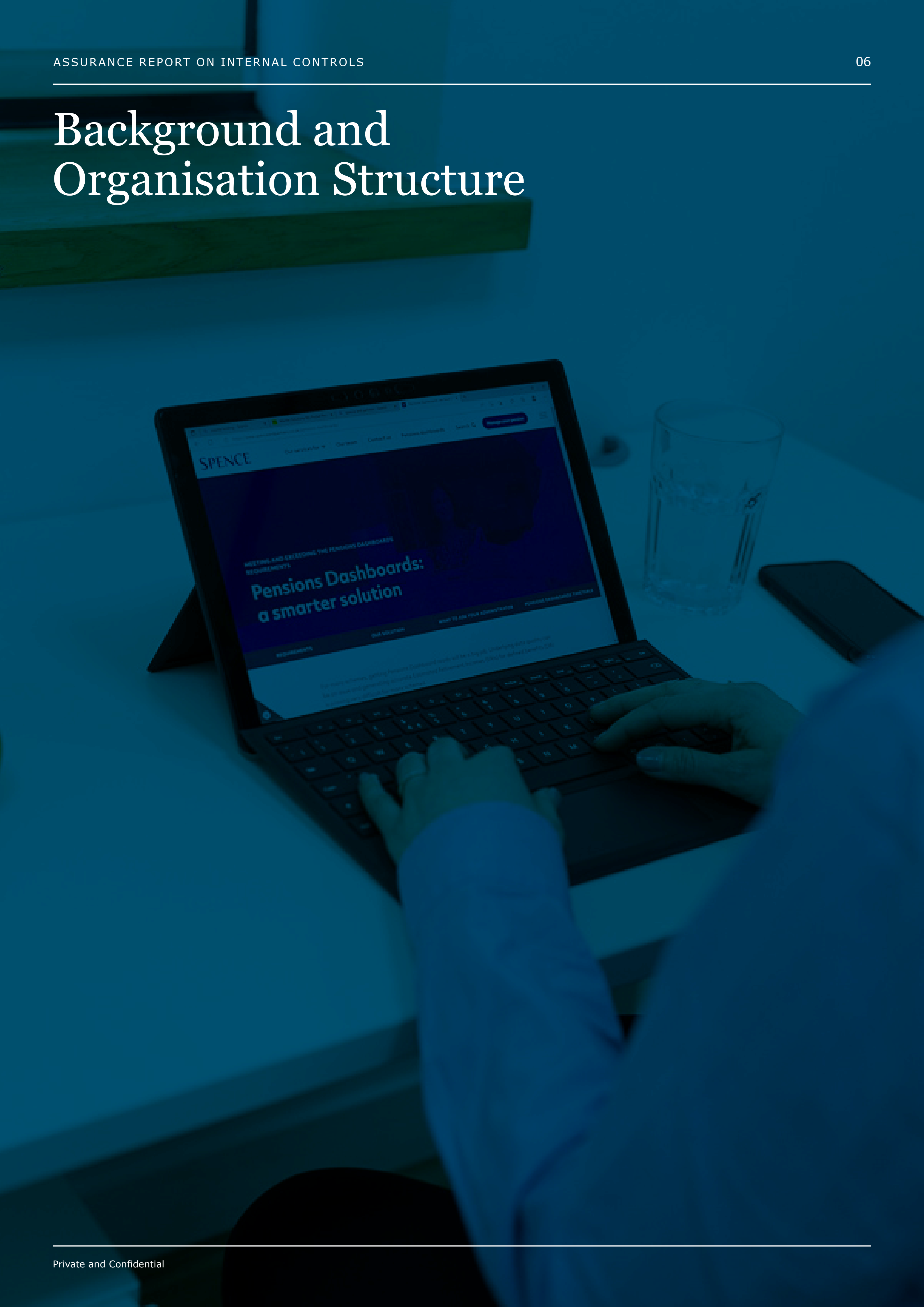
Effective pension scheme management is a pension scheme’s trustees’ responsibility. Our Trustee Advisory Practice delivers a range of practical solutions to trustees to help them comply with their legislative and regulatory responsibilities in a complex and ever-changing pensions landscape.

In addition to our work with trustees of ongoing schemes, we have developed specialist expertise in pension scheme termination work, and in particular managing schemes through PPF assessment periods. A specialist PPF/FAS team handles all aspects of the assessment process, including project management, administration and pension fund accounting. This expertise is ever more relevant to all schemes given The Pensions Regulator’s increasing focus on scheme record keeping and data.

Spence is one of only three firms appointed by the PPF in August 2016 to the Specialist Administration & Actuarial Services panel. We were also members of the predecessor panels since their inception in 2012Our pension administration service is controlled by a governance framework structured within a quality-controlled environment. The Directors of Spence are committed to providing the highest quality services to clients and maintaining a strong process, control and compliance environment throughout its practice areas.

This report provides the reader (including trustees, auditors and clients) with information and assurances about our processes and the strongly controlled environment that is in place to assist us in delivering high quality pension administration services to our diverse portfolio of schemes.

Background and Organisation Structure



Background and Organisation Structure

Spence was established in 2000, and is a wholly owned subsidiary of 3173 Limited ("the Group") which is majority owned by growth investor Synova LLP.

Spence provides full pension actuarial, consulting and administration services for over 80 schemes and advisory and support services to more than 100 trustee boards and sponsoring employers. Our clients' scheme sizes vary from less than £5m to over £500m. Most of our schemes are closed to accrual of future benefits.

Since our inception, we have advised and managed defined benefit pension schemes at varying stages of their development including ongoing schemes, schemes in the process of winding up and schemes in PPF and FAS assessment.

We have grown steadily since inception and the Group now employs 219 members of staff across seven offices in Belfast, Birmingham, Bristol, Glasgow, Leeds, London, and Manchester. Including Spence, there are five companies under the 3173 umbrella, as shown on the following page.

Our business structure and the quality of our staff give us access to a breadth of experience and range of services which compares favourably with any other local or national provider, whilst allowing us to offer a proactive and personalised service.

Spence is focused on the provision of excellent support services to employers and trustees operating defined benefit pension schemes. Our clients range from large UK PLCs and major Government bodies to small to medium-sized schemes, all of which require engaged and proactive advisers, actuaries and administrators.

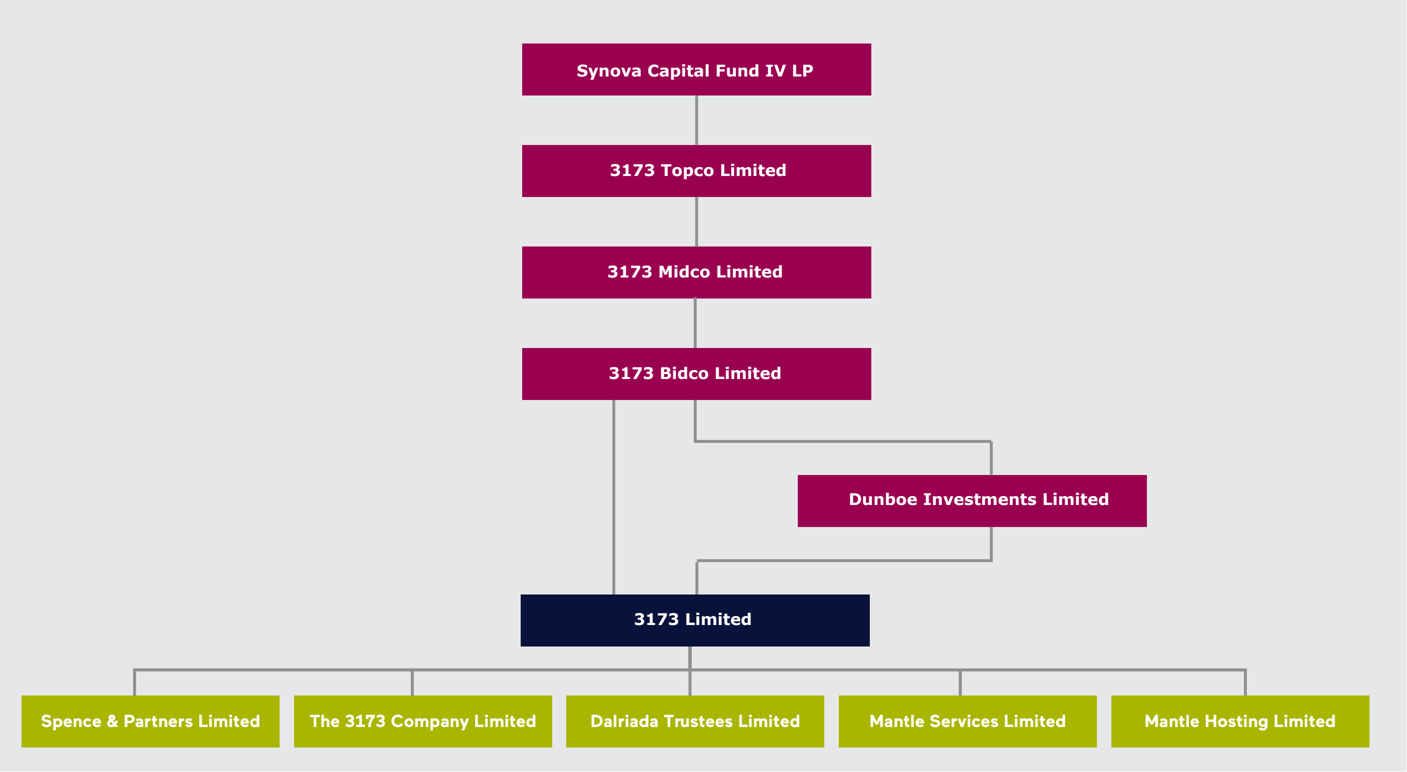
In 2003, Dalriada Trustees ("Dalriada") was established as a separate company to provide high quality independent professional trusteeship services to pension schemes in the United Kingdom. In 2011, Mantle Hosting Limited (formerly The Pensions Hosting Company Limited Limited) was established as an IT software business, developing and licensing an integrated pension administration and actuarial software application.

In 2014, Mantle Services Limited (formerly Veratta Limited), a privately-owned UK firm of data management, software development, information security and IT specialists was established with a focus on the pensions and financial services industry.

Our clients are based throughout the UK and Ireland.

Glasgow
Belfast
Leeds
Manchester
Birmingham
Bristol
London

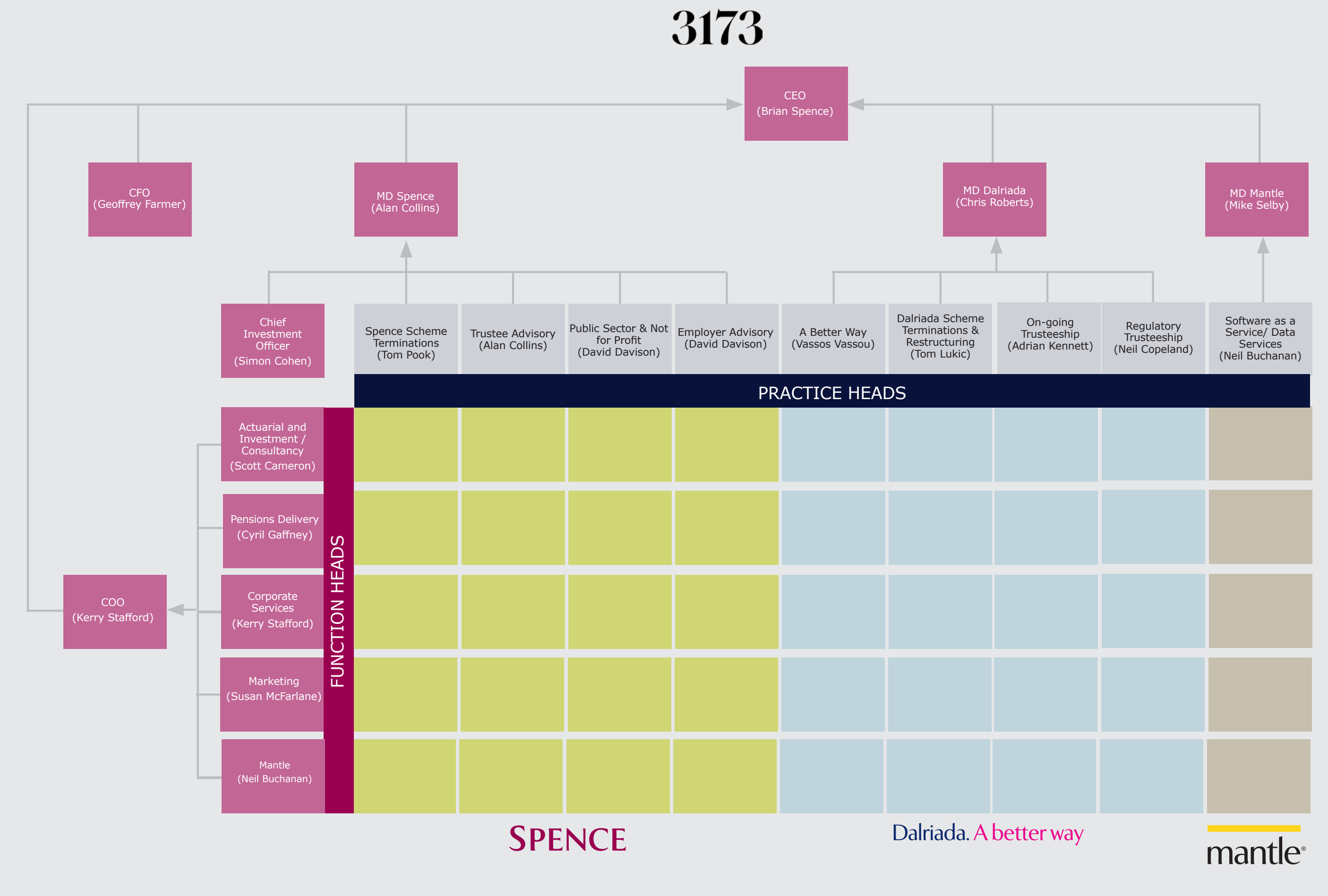
3173 Limited is the holding company for the Group. In 2022, 3173 announced an investment into its group of companies from growth investor Synova. The investment will consolidate the group's existing market-leading positions in pension scheme trustee services, unique pensions software, consultancy, administration, governance, actuarial and investment services and facilitate the next phase of the group's growth in an increasingly competitive pensions and financial technology industry. The following diagram shows the group's structure.



Under our Group's matrix management structure, Spence is able to draw on the experience of over 219 pension professionals across a range of disciplines. Specialist members of staff include actuaries, administrators, consultants, pension database experts, pension fund accountants, and project managers. The Group structure provides a flexibility which allows us to effectively manage resource levels to match variable workflows from clients, ensuring a consistency of service.

Our approach is driven by our belief that all schemes, regardless of budget, should be able to deliver employee benefits without putting strain on the employer. Our unique combination of award winning technology and market-leading servicing approach allows us to deliver improved decision making with tangible benefits.

Our structure is illustrated in the table below as a two-dimensional matrix.


3173
CEO (Brian Spence)
CFO (Geoffrey Farmer)
MD Spence (Alan Collins)
MD Dalriada (Chris Roberts)
MD Mantle (Mike Selby)
Chief Investment Officer (Simon Cohen)
Spence Scheme Terminations (Tom Pook)
Trustee Advisory (Alan Collins)
Public Sector & Not for Profit (David Davison)
Employer Advisory (David Davison)
A Better Way (Vassos Vassou)
Dalriada Scheme Terminations & Restructuring (Tom Lukic)
On-going Trusteeship (Adrian Kennett)
Regulatory Trusteeship (Neil Copeland)
Software as a Service/ Data Services (Neil Buchanan)
PRACTICE HEADS
FUNCTION HEADS
Actuarial and Investment / Consultancy (Scott Cameron)
Pensions Delivery (Cyril Gaffney)
Corporate Services (Kerry Stafford)
Marketing (Susan McFarlane)
Mantle (Neil Buchanan)
COO (Kerry Stafford)
SPENCE
Dalriada. A better way
mantle

Our Practice Heads across all of 3173's companies are responsible for all aspects of services to a particular market segment.

Practice Heads take overall responsibility for services to clients by drawing on specialist staff from within each of the Functions.

Each Function is managed by a Function Head, who controls all resources for client delivery and provides these to the businesses as a whole and practice areas as required. The most relevant Functions for this report are our Consultancy and Pensions Delivery functions.

The role of the Client Manager is key to our working relationship with clients. The Client Manager is the client's "champion" within Spence. From pension scheme trustees' point of view, they have assurance that there is one person with overall responsibility for their account. The Client Manager is supported by a client team drawn from across the functions of our business. The Function Heads and Client Managers have access to management information to enable them to plan and monitor progress on particular projects and against agreed fee budgets.

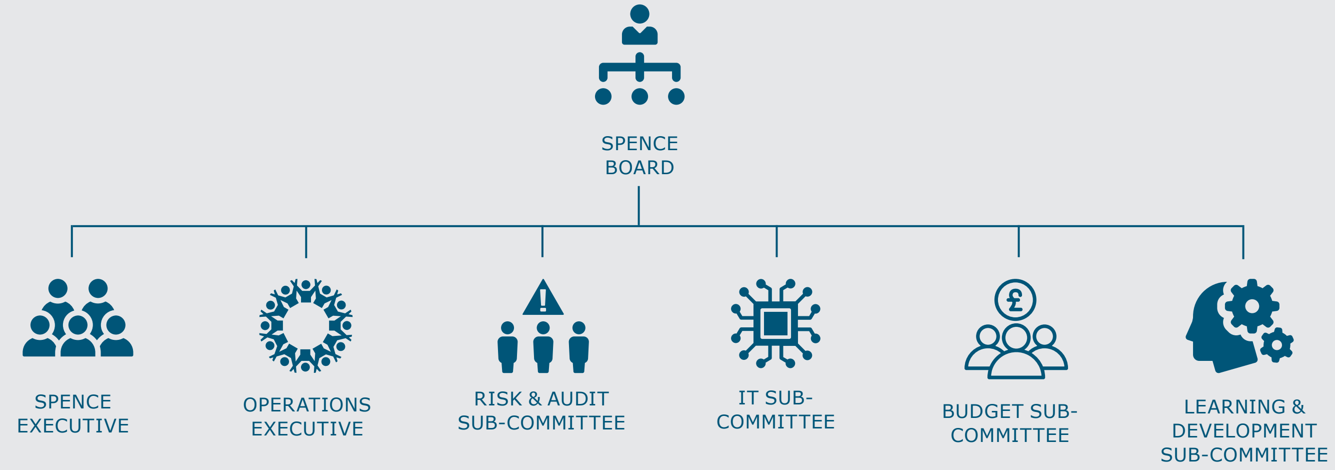
The separation between our Functions is not hard and fast. Although staff members are primarily associated with one Function, they can potentially perform a role in more than one Function, because we deliberately train staff to develop multiple skills.

In addition to the direct client servicing Functions, our Corporate Services Function contains internal finance, I.T., People & Culture, Risk and Audit and Business Support resources. Our Marketing, Communications and Business Development Function delivers promotional and sales support across the group.

The Consultancy and Pensions Delivery Function Heads report to Kerry Stafford, Chief Operating Officer. The Marketing Function Head reports jointly to Kerry Stafford and to our Chief Executive Officer, Brian Spence. The Practice Heads for Spence Scheme Terminations and the Chief Investment Officer report to Alan Collins, a Director of Spence. Our Practice Heads across all Companies report to Brian Spence.

Our statutory company boards meet quarterly and perform oversight and governance roles for each of the businesses and groups as a whole.

The Spence Board is supported by a number of advisory groups



- **Spence Executive:** external affairs and business development (meets quarterly).
- **Operations Executive:** coordination of resources and internal operations (meets monthly).
- **Risk & Audit Sub-Committee:** considers Group level risk and audit issues (meets quarterly).
- **IT Sub-Committee:** drives IT strategy for the Group (meets quarterly).
- **Budget Sub-Committee:** financial issues (meets quarterly).
- **Learning & Development Sub-Committee**

Pension Services

Pension Services

Spence provides a full range of pension administration and pension database services, operated within a quality-controlled environment.

Our pension administration team, within the Pensions Delivery Function, carries out all tasks and operations under a strict quality control and governance framework. We have procedures and checks in place to ensure the accuracy and quality of our service.

Spence recognises that its administration service is the interface between a pension scheme and its members; our pension administration team fully understands the importance of this. We never lose sight of the fact that the primary objective of a pension scheme is to provide benefits and information to its members in a timely manner. Pension administration is a core service for our business, rather than an adjunct to other services, and we are committed to a process of continuous improvement in terms of the services we provide to our clients.

A complete range of administration services are provided as a core and/or distinct element of our service including:

- calculation and communication of benefit entitlements;
- processing of benefit settlements;
- cash management - operation of the scheme bank account, cashflow analysis, investment and disinvestment of funds as appropriate;
- production of formal pension scheme annual report and accounts by our specialist pension fund accounting team;
- processing pension payroll; and
- a comprehensive data and benefit audit reporting system to comply with The Pensions Regulator’s record keeping requirement.

Management Systems and Controls

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

STRUCTURE

A key component of our approach to quality is the separation of responsibility within our Group between the Practice Head, who is responsible for identifying the needs of our clients and strategically developing our service to meet these needs, and our Function Heads (Consultancy and Pensions Delivery Functions) who manage the resources and day-to-day delivery of services.

PROCEDURES

Our procedures are owned by the relevant Function Head and evidenced in a series of control documents available on our intranet site. Where relevant, all documents are managed through our formal Information Security Management System (“ISMS”). Spence’s ISMS is externally certified under ISO/IEC 27001:2013 - Information technology - Security techniques - Information security management systems - Requirements.

Most procedures are automated as workflows on our in-house workflow system, which also captures and measures our performance against Service Level Agreements.

CONTENT MANAGEMENT

All procedures, documents, records and information are managed within an extensively developed SharePoint implementation with version control.

All colleagues have access to a wide variety of technical information sources.

CHECKING

There are strict checking procedures for all calculations and correspondence with trustees, members and third parties.

Checklists are completed to ensure that all the required steps are followed. All calculations are peer reviewed by a senior administrator ("the checker") along with the checklist to ensure there are no errors or omissions.

All approvals for calculations and correspondence are held within our workflow system.

SERVICE LEVEL AGREEMENTS

Traditionally, a Service Level Agreement ("SLA") for pension administration focuses on carrying out an action (e.g. responding to an individual item of post or an email within a defined timescale). The creation of an "action" becomes more of an end in itself, rather than meeting the needs of a member.

Our monitoring is around whole events (i.e. a member's death) rather than actions. The traditional approach would have been to allow a turnaround of one day, say in respect of any incoming correspondence or trigger for action.

A true measure of the performance of the trustees, and of us as administrators, is the time taken for the death benefits to actually be paid.

A member (or in the event of their death, their dependants) will not really place great value on a particular letter having been answered within one day. However, they will want to know when their benefits will be settled.

The administration team aims to carry out services and tasks accurately and efficiently to meet or exceed SLAs. SLAs are continuously monitored internally, and reported externally to trustees, in the form of a Stewardship report. The report details the tasks undertaken during the relevant period and whether or not the SLAs have been met. This allows the trustees to monitor the performance against the SLA.

All key subservice providers are ISO27001:2013 accredited. This is in line with business processes and ensures the protection of all assets accessible by providers and to maintain an agreed level of information security and service delivery in line with supplier agreements. In line with our company policies periodic reviews are held with all key subservice providers and where applicable site visits are conducted at regular intervals.

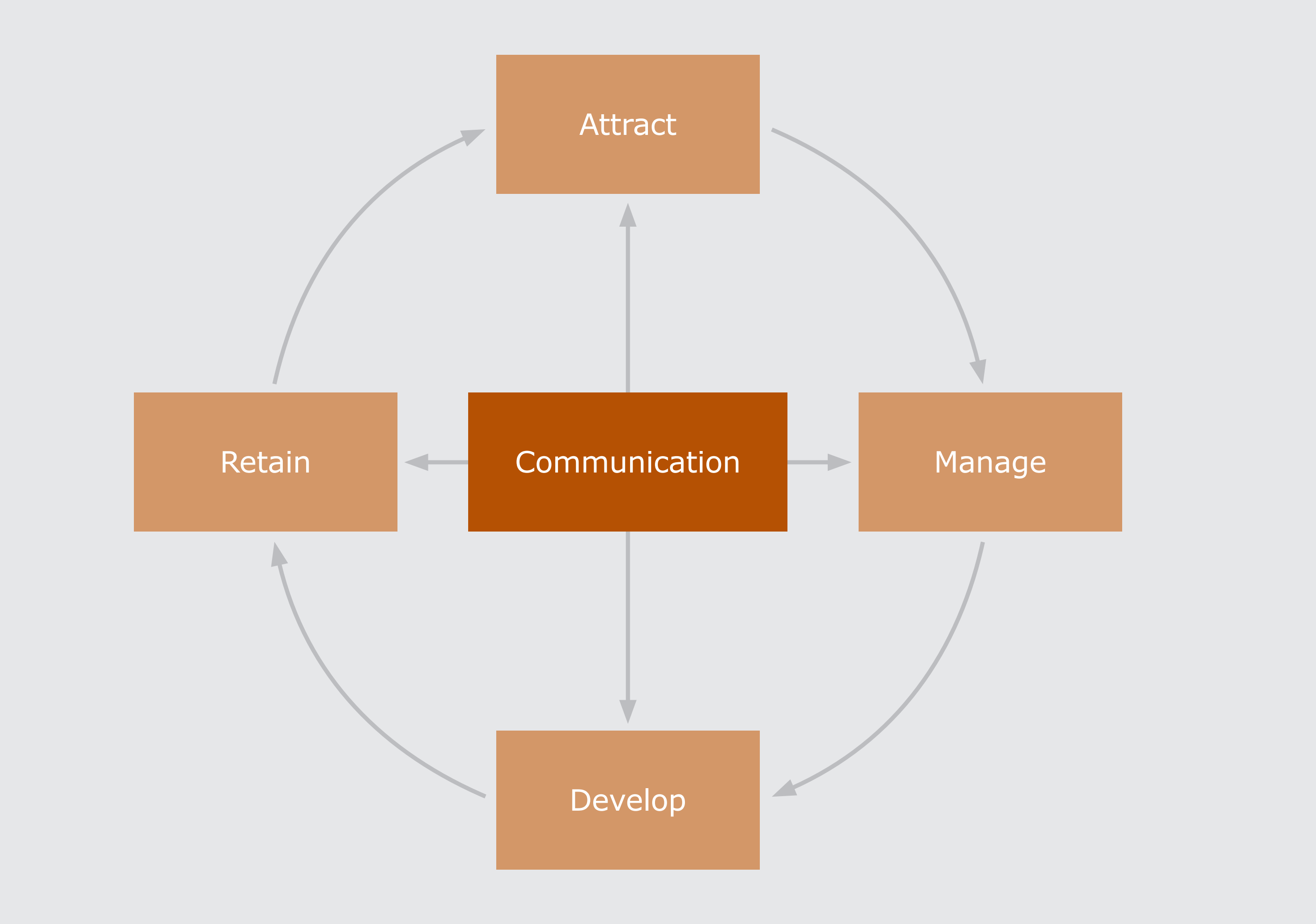
ELECTRONIC DOCUMENT AND TASK MANAGEMENT

To underpin our workflow management system, we have implemented Microsoft SharePoint software, enabling us to introduce comprehensive electronic document management. All correspondence for our clients is scanned and available for searching and retrieval. Our workflow system enables client managers to monitor closely the turnaround times on individual pieces of work, the total amount of outstanding work and where any particular job is at any moment in time. Additionally, Spence has developed advanced reporting tools so that detailed activity and performance information can be extracted at any point in time and, indeed, forms the basis of our standard Stewardship Reporting.

AUDIT

Compliance with our procedures is subject to internal audits and external audits (AAF 01/20). The Information Security Management System (ISMS) is subject to separate external audit for ISO 27001 purposes.

Our organisational goal is to provide interesting, worthwhile and healthy careers for all our employees. Our People & Culture team works in partnership with our Function Head Group to deliver the People & Culture strategy of Attract, Manage, Develop, Retain and supports the overall strategy of the Company.



- **Attract:** we recruit the highest calibre colleagues through robust and challenging recruitment and security exercises to ensure our clients are supported by qualified, professional, and credible employees.
- **Manage:** we actively manage our employees in a collaborative manner and all our operational employees engage with our performance management review process on an ongoing basis. The results of these reviews are integrated with our salary and bonus system, rewarding high performance against agreed goals aligned with the needs of our business and our clients.
- **Develop:** we adopt a supported Learning and Development approach working with our employees through a combination of in-role learning, professional qualifications, formal study plans, and mentoring, to enhance the capability of our employees and enhance our client service. All our operational managers have undertaken management development training specific to our company and industry.
- **Retain:** at the heart of our processes, is effective communication. Through our engaging culture we have enjoyed high retention levels which ensure consistency of delivery for our clients.

In support of the above:

- We have a dedicated Learning & Development Sub-Committee.
- We have clearly defined and documented policies and procedures governing the services we provide; these are communicated clearly to all relevant colleagues.
- Our policies and procedures are regularly reviewed with a view to identifying and implementing continuous improvements.
- Changes to our policies and procedures are clearly communicated to all colleagues and relevant contractors.
- Compliance with our standards and relevant policies and procedures is regularly audited.

CULTURE

Our culture has a vital role to play in the delivery of our vision and our achievement of quality. Our cultural ethos and principles are outlined in our 'Above All Else' document https://www.3173.co.uk/wp-content/uploads/2021/03/3173-Culture-Brochure.pdf. We embed our culture in everything we do and it is lived out by our employees.

KNOWLEDGE MANAGEMENT

John Wilson is our Head of Technical Research and Policy, and he is also our Knowledge Management Co-ordinator ("KMCO").

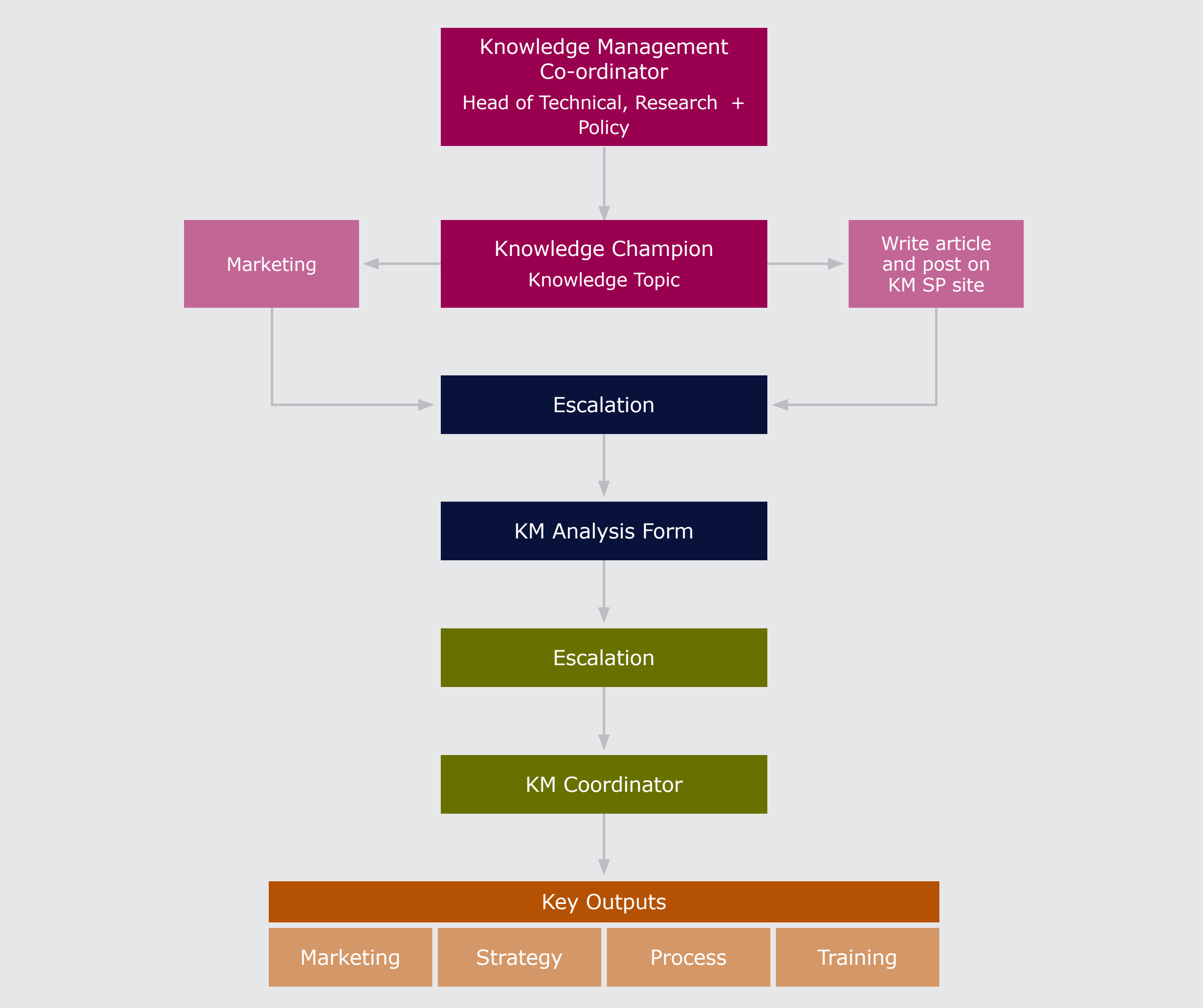
The KMCO has responsibility for coordinating the Knowledge Management "KM" process across the Group. This involves, in addition to production of internal and external KM output, reviewing the output produced by KM Champions, assessing whether appropriate analysis has been undertaken, deciding whether further training or development should follow on from the output, and reporting to the Risk & Audit Committee and the Board of Directors. The KMCO oversees the overall production of KM information, as well as production and facilitation of information. The KMCO also chairs our Learning & Development Sub-Committee.

The role of the KMCO includes, but is not limited to, the following duties:

- Keeping the Group up to date with developments in pensions law and practice.
- Management and ownership of the KM activity across the business including a programme plan of projects, training and other activities to ensure control of delivery into the business.
- Conveying understanding of the strategic importance of the KM function for the business as a whole.

- Encouraging engagement and input into the KM function by all members of staff, whether or not they are Champions.
- Assessing the use and application of the knowledge and information shared on the system, and seeking to improve its presentation to ensure user friendly outputs.
- Reviewing the work of the Champions, ensuring that they are regularly updating the detail and fulfilling their KM responsibilities.
- Promoting the development of alternative approaches to communications, collaboration and information technologies that effectively support the KM processes, within and between organisations and clients, both internal and external.
- Meeting with and reporting to the Risk & Audit Committee regularly, with appropriate updates when required to Practice and Function Heads Groups, as well as the Board of Directors.
- Helping to promote the thought leadership credentials of the business through PR activities, membership of industry trade associations and leading responses to government and regulator consultation papers and calls for evidence.

The below diagram outlines our process:


Knowledge Management Co-ordinator

Head of Technical, Research + Policy

Marketing

Knowledge Champion

Knowledge Topic

Write article and post on KM SP site

Escalation

KM Analysis Form

Escalation

KM Coordinator

Key Outputs

Marketing

Strategy

Process

Training

We appoint Knowledge Subject Matter Champions who are experts in particular technical areas and develop the Group’s and our clients’ understanding on key updates.

Information Security

Information security is of paramount importance to our organisation. We are committed to protecting information from a wide range of threats to preserve the confidentiality, availability and integrity of that information, to ensure business continuity and to minimise business risk for us, and for our clients.

Our Group has engaged a CESG Listed Adviser Scheme ("CLAS") consultant to provide information assurance advice in relation to our systems and we have implemented all recommendations.

Since December 2011, Spence has been successfully certified under the International Organisation for Standardisation, ISO 27001, an internationally recognised standard for information security management. Spence was recertified to ISO27001:2013 in 2017 and completed triennial recertification in 2020.

ISO27001:2013 is the international touchstone for effective, secure information management practices that protect organisations, and their clients, and ensure their compliance with data protection, privacy and computer misuse regulations. The use of this standard primarily ensures business continuity, minimising damage by preventing and reducing the impact of security incidents.

The security practices, policies and technical and physical controls adopted by Spence to comply with the ISO 27001 accreditation are essential to ensure the safe and secure deployment of IT systems and services, and to protect the interests of the Group's employees and its clients.

Our information security policy outlines our:

Commitment to information security, including how we comply with existing data protection legislation;

Protection of key assets: information, personnel, technology, processes;

Risk management process;

Training and awareness of staff and third parties;

Reporting and resolution of information security breaches; and

Business Continuity Management System.

Our Data Protection Policy sets out how Spence handles personal information in compliance with the UK General Data Protection Regulation and Data Protection Act 2018 ("GDPR"). It outlines:

- How we recognise that the correct and lawful processing of personal data is important and integral to our successful operations and to maintaining the trust of the persons/organisations we deal with. We fully endorse and adhere to the principles set out by the GDPR.
- We are registered with the Information Commissioner to process 'personal data' and 'special category – sensitive - personal data.'
- We are named as a data controller under the register kept by the Information Commissioner in accordance with the GDPR.
- Spence acts as data processor in relation to the handling of the personal data and sensitive personal data of the persons/organisations we deal with. The persons/organisations providing the personal data to Spence are the data controller in such circumstances for the GDPR.
- We ensure that information held on our computer systems and in paper filing systems is secure to guard against unauthorised or unlawful processing or accidental loss, destruction of, or damage to, personal data. In order to carry out our business, we may receive information about individuals from others or give information to others, but can only do this in accordance with the law. Any third parties to whom we pass personal data are also required to comply with the GDPR as data processors. At all times the persons/organisations that initially passed the personal data to Spence shall remain the data controllers.
- We only collect and record personal information that is necessary to carry out its purpose, nothing more. The information that we record is based on fact and, where opinion is recorded, it is relevant and backed up by evidence. We ensure that the storage and processing of personal information is properly communicated to data subjects, including information on their rights in relation to the regulations. We also review the quality of the information of the data that we hold to ensure it is accurate and relevant and securely dispose of information once it is no longer lawfully required.

As part of the staff induction process, all staff must complete an online Data Protection Course within the first two weeks of their employment. This is valid for two years, at which point a renewal is issued and this must be completed within two weeks.

DATA SERVICES

We include information about our lawful basis for processing data (or bases, if more than one applies) in our privacy notice.

Under the transparency provisions of the GDPR, the information we would be required to give includes:

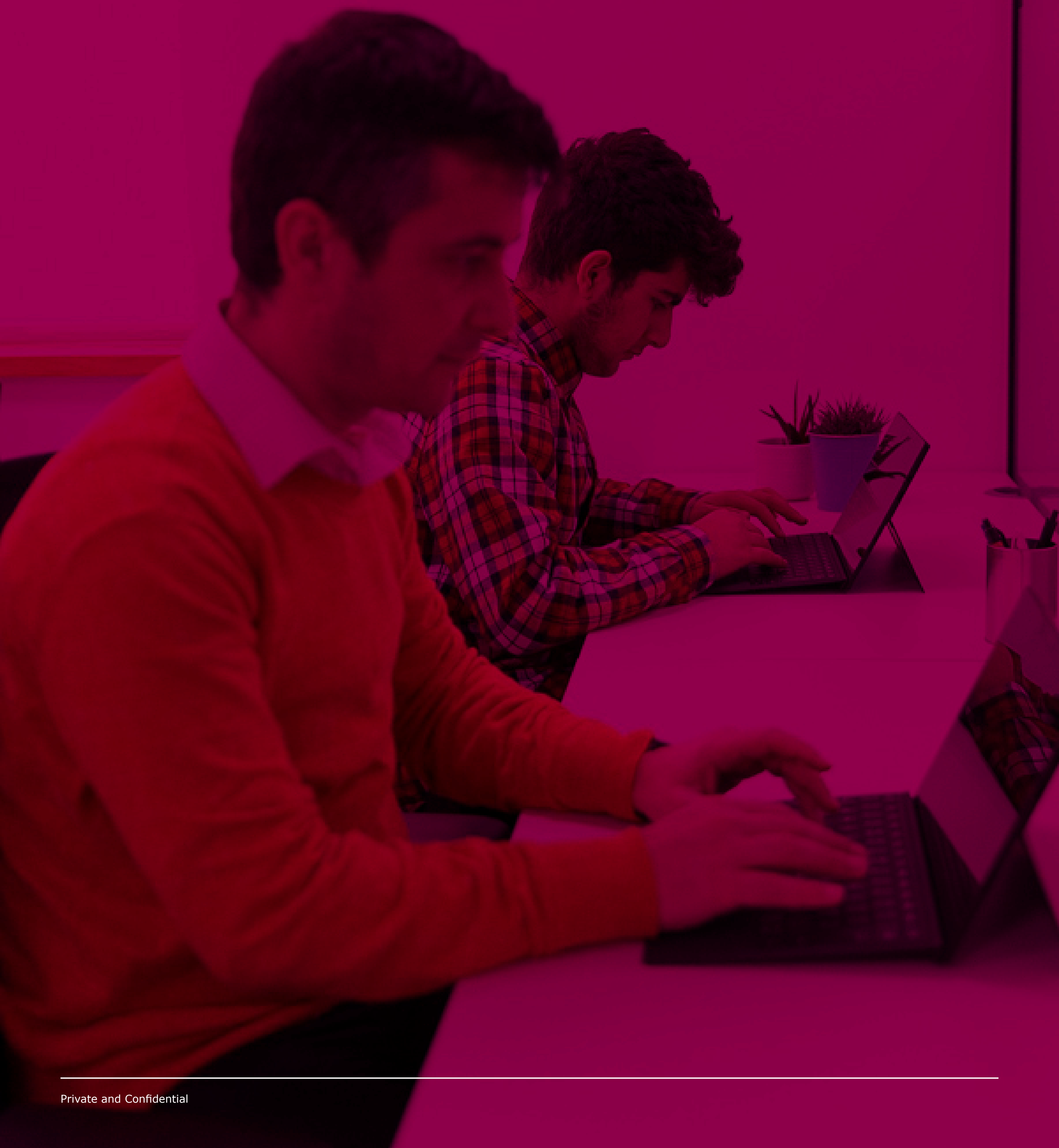
- our intended purposes for processing personal data, and
- the lawful basis for the processing. This would apply whether we collect personal data directly from the individual, or if it is collected from another source.

We provide the privacy information to individuals at the time we collect their personal data.

Our communications use plain language, are concise, transparent, intelligible and easily accessible. We communicate directly with individuals and also use our Member Portal, as an additional way of providing information (providing a multi-layered approach).

We regularly review and where necessary, update our privacy information and where needed, we would bring any new uses of an individual's personal data to their attention. We would also provide members with the contact details of our organisation, the contact details of our data protection officer together with the purpose of processing of their data. Particularly for communications with trustees, we will use anonymised communications to protect member data (e.g. Stewardship Reports). We also ensure password protection and secure online sharing of documents, including trustee papers, which avoids the need for storing and sharing of multiple hard copies.

Risk Management



Risk Management

Our risk assessment process involves identifying risk scenarios based on our key information assets. Associated threats to these assets are identified, along with the vulnerabilities that might be exploited by the threats.

Our Group Risk and Compliance Focus Group (GRC) meets quarterly and analyses risk scenarios.

The business impact and consequences of each risk are assessed on their consequences in terms of loss of confidentiality, integrity, or availability. This is scored and multiplied by a risk rating for business operational impact (severity impact), likelihood (probability score) and the extent to which it is business critical, providing an overall risk score. Identified risks are analysed and evaluated against risk acceptance criteria. Once risks have been identified and assessed, techniques to manage risk fall into one or more of these categories:

AVOIDANCE (ELIMINATION)

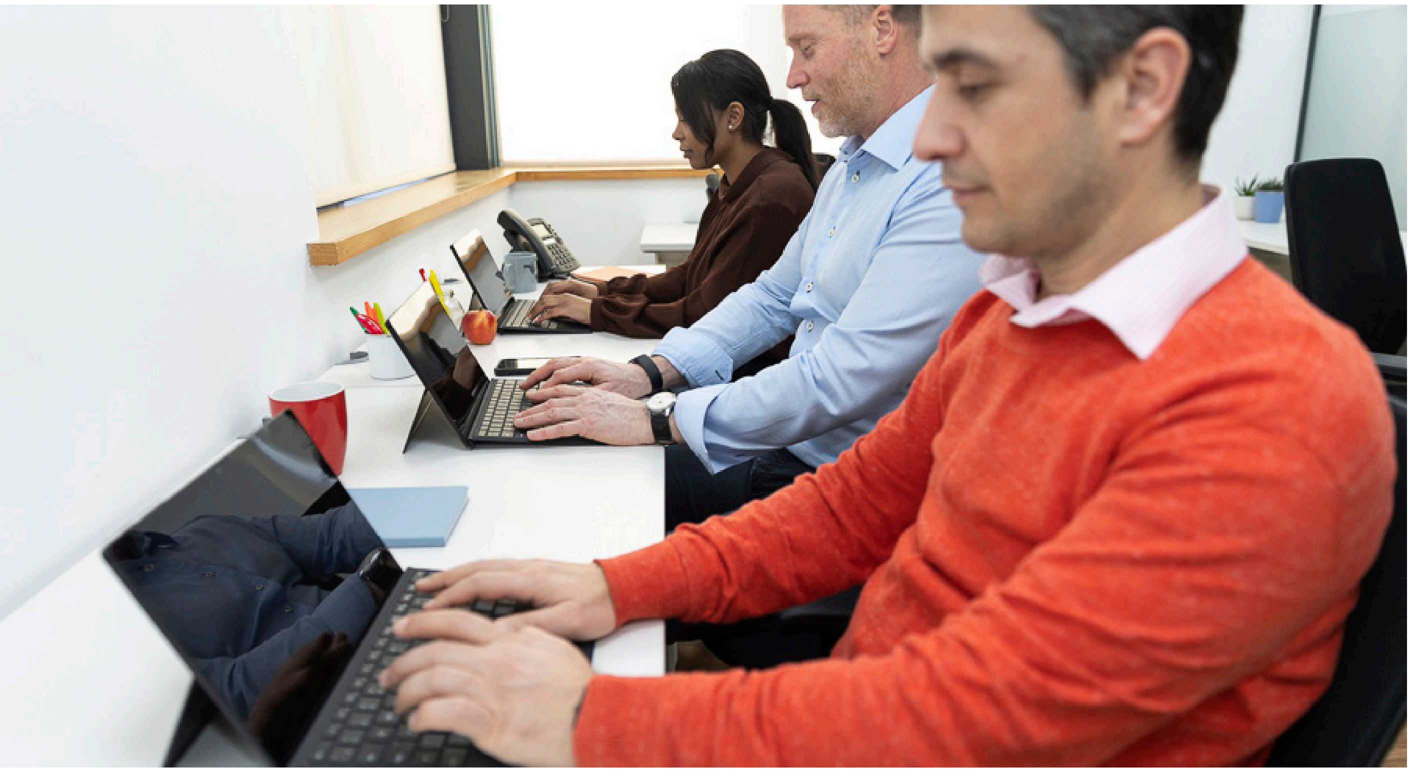
REDUCTION (MITIGATION)

RETENTION (ACCEPTANCE)

TRANSFER (INSURANCE)

Risk Treatment Plans are drawn up to provide the basis for knowingly and objectively accepting risks or implementing the required counter-measures. The Risk Treatment Plans are escalated and formally approved where appropriate.

The Risk Register is reviewed at planned intervals by our GRC to reflect changes in the underlying environment.



Information Technology

Information Technology

Spence’s IT infrastructure is a combination of Software as a Service “SaaS” from Office 365 and Infrastructure as a Service “IaaS” from Microsoft’s Secure Azure Cloud.

Spence has an in-house team of experts who manage and maintain Office 365 and Azure; this is complemented with a managed service provider offering.

Spence also utilises Mantle®, an innovative web application provided by Spence’s sister company, Mantle Hosting Limited.

Our voice network is also hosted within Office 365 on Microsoft Teams, with only end user devices held onsite.

Network Infrastructure

Spence has upgraded its core network to a highly resilient and secure MPLS offering.

Private connectivity exists into Office 365 and Azure via ExpressRoutes which are linked to the core network. This ensures that all data to Office 365 and Azure transits over highly secure private links which are never exposed to public internet.

Security

Our IT infrastructure is protected by a range of security measures within our ISO 27001 framework including:

- Secure, resilient perimeter firewalls with enhanced protection and threat mitigation.
- Regular CESG CHECK penetration testing to ensure compliance with HMG policy.
- 24/7 Azure Sentinel and CloudApp Security Monitoring
- Privileged Identity Management, Conditional Access and Multi Factor Authentication

SharePoint

We use SharePoint Online as a central resource for document management . Scheme documentation, member correspondence and internal function process documents are worked on and stored in this repository. Security permissions are in place to ensure that no conflicts of interest occur across our clients, and sensitive documents are managed accordingly.

Backup and Recovery

Office 365 SaaS applications are managed by Microsoft, whereby Spence simply consumes the service. This

transfers the responsibility for backup and restoration of the application to Microsoft.

Azure workloads are protected with daily backup within Azure whilst Disaster Recovery “DR” protection is handled by replication to a secondary Azure Datacentre; this ensures that the company is not exposed to a Datacentre failure.

Administration Database

Mantle is the most efficient pension administration system available in the market today and was developed by our sister company, Mantle Hosting Limited, to meet developing industry needs. Functionality includes fully automated benefit calculations, document storage, automated workflows, daily actuarial valuations, treasury and data audits.

Spence also utilises a separate Microsoft SQL based application for certain one-off projects and is in the process of decommissioning this application for ongoing schemes.

Email Archiving

Spence has maintained an online archive of all emails sent and received since it was founded in 2000. Any email can be accessed within a matter of seconds using our email archiving software, Mimecast.

Mimecast is an online security and email archiving platform hosted in the Cloud. This serves as the first line of defence for email with threat analysis, intelligence and exploit mitigation.

All mailboxes are replicated to Mimecast in read only format and cannot be deleted.

Mimecast also provides a continuity feature whereby email can still be sent and received should an outage occur with the backend Office 365 platform.

End User Computing

We operate a number of control activities with respect to our key systems and applications that include:

- All users are allocated a unique network User ID and Password. Access to applications is achieved with the use of multifactor authentication and conditional access policies.
- Cryptographic controls for protection of information is developed and implemented by all staff.
- Changes to access rights are logged and recorded by the internal IT department.
- Removable media devices are rarely used and in the event that a removable media device is required, the internal IT representative is responsible for procurement, encryption, and key management.
- The Group use an industry standard sharing application ShareFile. Sensitive information transmitted by e-mail must be sent via ShareFile. More recently external access has been granted via Azure with guest access using two factor authentication. All new external access is granted using this method.
- External users have browser only access to documents; are unable to download. This is set by a policy within Azure.
- Azure Site Recovery (ASR) is used as our disaster recovery infrastructure, end to end encryption is employed to ensure security data transfer.
- Virtual machines and databases are backed up using Azure Backup and are stored securely in Azure.
- End devices are protected against Malware and viruses via Windows Defender and Advanced Threat Protection.
- All devices are managed via industry leading Mobile Device Management “MDM” platforms. MDM applies corporate polices to all company endpoints to ensure compliant with company security standards.
- Conditional based access control security measures are applied to all devices to ensure a device is compliant before it can access company data.
- Spence also has the ability to revoke any company owned data from any corporate device with immediate effect, should the need arise.

Report from the Directors of Spence & Partners Limited

Report from the Directors of Spence & Partners

As Senior Management of Spence & Partners (‘the Service Organisation’) we are responsible for the identification of Control Objectives relating to the provision of pension administration services, pension data audit and pension benefit audit services for pension scheme trustees by the Service Organisation and the design, implementation and operation of the Service Organisation’s Control Activities to provide reasonable assurance that the Control Objectives are achieved.

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

The accompanying description has been prepared for User Entities who have used the pension administration services, pension data audit and pension benefit audit services for pension scheme trustees and their auditors who have a sufficient understanding to consider the description, along with other information including information about Control Activities operated by User Entities themselves.

We have evaluated the fairness of the description and the design suitability of the Service Organisation’s Control Activities in accordance with the Technical Release AAF 01/20 (‘AAF 01/20’), issued by the Institute of Chartered Accountants in England and Wales, and the Control Objectives for pension administration services, pension data audit and pension benefit audit services for pension scheme trustees set out in AAF 01/20 and the International Standard on Assurance Engagements 3402 (‘ISAE 3402’), issued by the International Auditing and Assurance Standards Board.

We confirm that:

a. The accompanying description in sections 3 to 5 fairly presents the Service Organisation’s pension administration services, pension data audit and pension benefit audit services throughout the period 1 January 2022 to 31 December 2022. In addition to the Control Objectives specified in AAF 01/20, the criteria used in making this statement were that the accompanying description:

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

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

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

b. The Control Activities related to the Control Objectives stated in the accompanying Description were suitably designed and operated effectively throughout the period 1 January 2022 to 31 December 2022. The criteria used in making this statement were that:

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

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

iii. The Control Activities were consistently applied as designed.

Alan Collins

Alan Collins Director

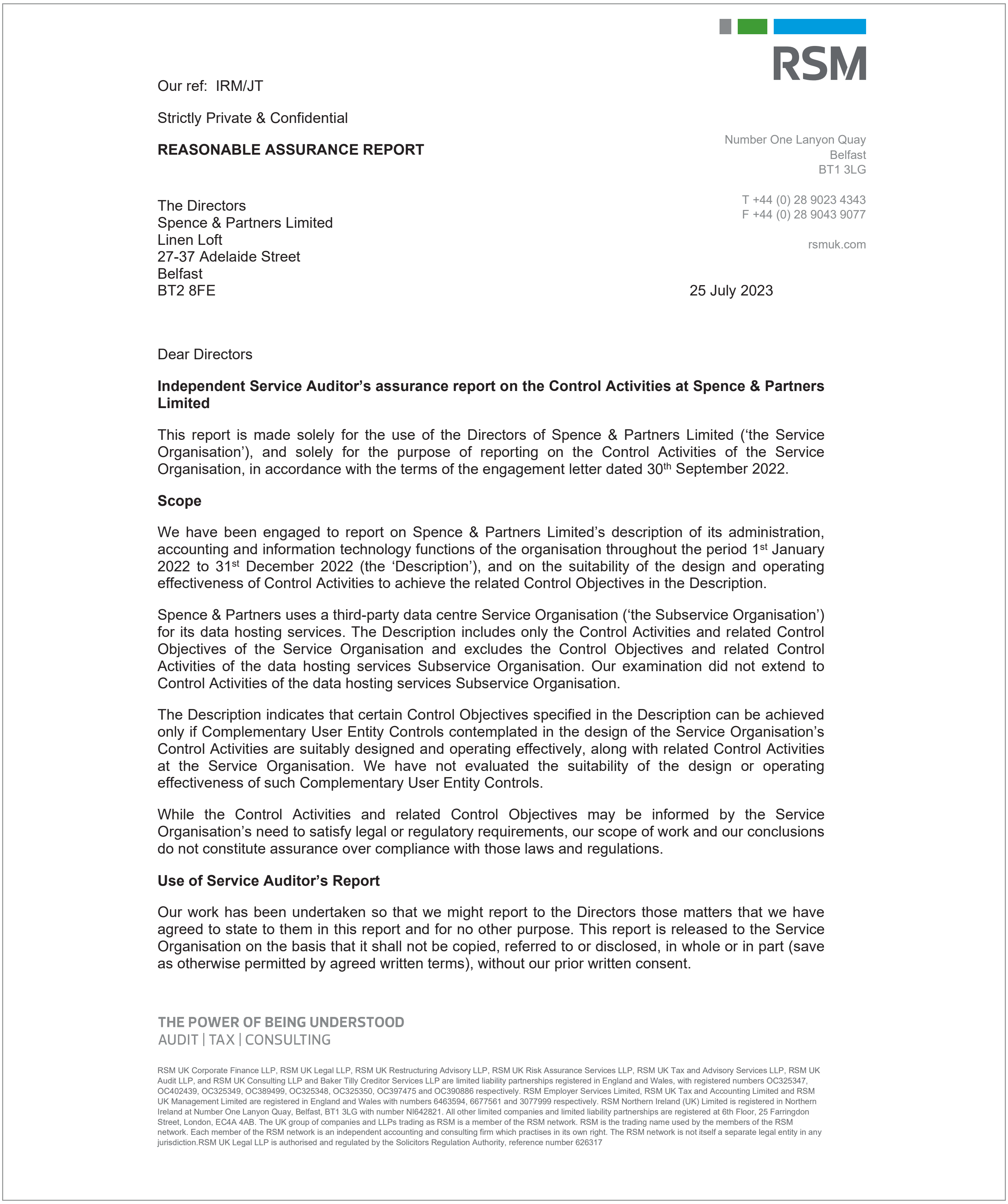
Signed on behalf of the Board of Directors

Spence & Partners Limited

Date: 26 July 2023

Independent Assurance Report

Independent Assurance Report



RSM

Our ref: IRM/JT

Strictly Private & Confidential

REASONABLE ASSURANCE REPORT

Number One Lanyon Quay
Belfast
BT1 3LG

T +44 (0) 28 9023 4343
F +44 (0) 28 9043 9077

rsmuk.com

The Directors
Spence & Partners Limited
Linen Loft
27-37 Adelaide Street
Belfast
BT2 8FE

25 July 2023

Dear Directors

Independent Service Auditor's assurance report on the Control Activities at Spence & Partners Limited

This report is made solely for the use of the Directors of Spence & Partners Limited ('the Service Organisation'), and solely for the purpose of reporting on the Control Activities of the Service Organisation, in accordance with the terms of the engagement letter dated 30th September 2022.

Scope

We have been engaged to report on Spence & Partners Limited's description of its administration, accounting and information technology functions of the organisation throughout the period 1st January 2022 to 31st December 2022 (the 'Description'), and on the suitability of the design and operating effectiveness of Control Activities to achieve the related Control Objectives in the Description.

Spence & Partners uses a third-party data centre Service Organisation ('the Subservice Organisation') for its data hosting services. The Description includes only the Control Activities and related Control Objectives of the Service Organisation and excludes the Control Objectives and related Control Activities of the data hosting services Subservice Organisation. Our examination did not extend to Control Activities of the data hosting services 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 Service Organisation's Control Activities are suitably designed and operating effectively, along with related Control Activities at the Service Organisation. We have not evaluated the suitability of the design or operating effectiveness of such Complementary User Entity Controls.

While the Control Activities and related Control Objectives may be informed by the Service Organisation's need to satisfy legal or regulatory requirements, our scope of work and our conclusions do not constitute assurance over compliance with those laws and regulations.

Use of Service Auditor's Report

Our work has been undertaken so that we might report to the Directors those matters that we have agreed to state to them in this report and for no other purpose. This report is released to the Service Organisation on the basis that it shall not be copied, referred to or disclosed, in whole or in part (save as otherwise permitted by agreed written terms), without our prior written consent.

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

RSM UK Corporate Finance LLP, RSM UK Legal LLP, RSM UK Restructuring Advisory LLP, RSM UK Risk Assurance Services LLP, RSM UK Tax and Advisory Services LLP, RSM UK Audit LLP, and RSM UK Consulting LLP and Baker Tilly Creditor Services LLP are limited liability partnerships registered in England and Wales, with registered numbers OC325347, OC402439, OC325349, OC389499, OC325348, OC325350, OC397475 and OC390886 respectively. RSM Employer Services Limited, RSM UK Tax and Accounting Limited and RSM UK Management Limited are registered in England and Wales with numbers 6463594, 6677561 and 3077999 respectively. RSM Northern Ireland (UK) Limited is registered in Northern Ireland at Number One Lanyon Quay, Belfast, BT1 3LG with number NI642821. All other limited companies and limited liability partnerships are registered at 6th Floor, 25 Farringdon Street, London, EC4A 4AB. The UK group of companies and LLPs trading as RSM is a member of the RSM network. RSM is the trading name used by the members of the RSM network. Each member of the RSM network is an independent accounting and consulting firm which practises in its own right. The RSM network is not itself a separate legal entity in any jurisdiction.RSM UK Legal LLP is authorised and regulated by the Solicitors Regulation Authority, reference number 626317

RSM

This Service Auditor’s Report is designed to meet the agreed requirements of the Service Organisation and particular features of our engagement determined by their needs at the time. This report should not therefore be regarded as suitable to be used or relied on by any other party wishing to acquire any rights against RSM UK Risk Assurance Services LLP for any purpose or in any context. Any party other than the Service Organisation which obtains access to this report or a copy and chooses to rely on this report (or any part of it) will do so at its own risk. To the fullest extent permitted by law, RSM UK Risk Assurance Services LLP will accept no responsibility or liability in respect of this report to any other party and shall not be liable for any loss, damage or expense of whatsoever nature which is caused by any person’s reliance on representations in this report.

We permit the disclosure of our Service Auditor’s Report, in full only, to current and prospective customers of the Service Organisation using the Service Organisation’s pension administration services and related information technology ("User Entities"), and to the auditors of such User Entities, to enable User Entities and their auditors to verify that the Service Auditor’s Report has been commissioned by the Directors of the Service Organisation and issued in connection with the Control Activities of the Service Organisation without assuming or accepting any responsibility or liability to them on our part.

Service Organisation’s responsibilities

The Service Organisation is responsible for:

- preparing the Description on pages 6 to 26 and 32 to 61 and the accompanying Directors Statement set out on pages 25 to 27 including the completeness, accuracy and method of presentation of the Description and the Management Statement;
- providing the Service Organisation’s administration, accounting and information technology activities, covered by the Description;
- specifying the Criteria and stating them in the Description;
- identifying the risks that threaten the achievement of the Control Objectives; and
- designing, implementing and effectively operating Control Activities to achieve the stated Control Objectives.

The Control Objectives stated in the Description on pages 6 to 26 include the internal Control Objectives developed for the Service Organisation’s administration, accounting and information technology activities as set out in ICAEW Technical Release AAF 01/20.

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 Standards on Assurance Engagements 3000 (Revised) and ICAEW Technical Release AAF 01/20. Those standards and guidance require that we comply with ethical requirements and plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the Description is fairly presented and the Control Activities were suitably designed and operating effectively to achieve the related Control Objectives stated in the Description.

An assurance engagement to report on the Description and design of Control Activities at a Service Organisation involves performing procedures to obtain evidence about the presentation of the Description and the suitability of design of the Control Activities. Our work involved performing procedures to obtain evidence about the presentation of the Description of the Service Organisation pension administration activities and related information technology and the design and operating effectiveness of those Control Activities. 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

RSM

Description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the Description and the suitability of the Control Objectives stated therein.

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

Inherent Limitations

The Service Organisation's Description is prepared to meet the common needs of a broad range of User Entities and their auditors ('User Organisations') and may not, therefore, include every aspect of the Service Organisation's pension administration services and related information technology that each individual User Entity may consider important in its own particular environment. Also, because of their nature, Control Activities at a Service Organisation may not prevent or detect and correct all errors or omissions in processing or reporting transactions.

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 the suitability of the design or operating effectiveness of the Control Activities would be inappropriate.

Opinion

In our opinion, in all material respects, based on the Criteria described in the Service Organisation's Director's Statement on pages 25 to 27:

(a) the Description on pages 6 to 26 and 32 to 61 fairly presents the Service Organisation's pension administration services as designed and implemented throughout the period from 1st January 2022 to 31st December 2022;

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

Description of tests of Control Activities

The specific Control Activities tested and the nature, timing and results of those tests are detailed on pages 32 to 61.

RSM UK Risk Assurance Services LLP

RSM UK Risk Assurance Services LLP
Belfast
25 July 2023

Summary of Control Objectives

SPENCE
MEETING AND EXCEEDING THE PENSIONS DASHBOARDS REQUIREMENTS
Pensions Dashboards: a smarter solution

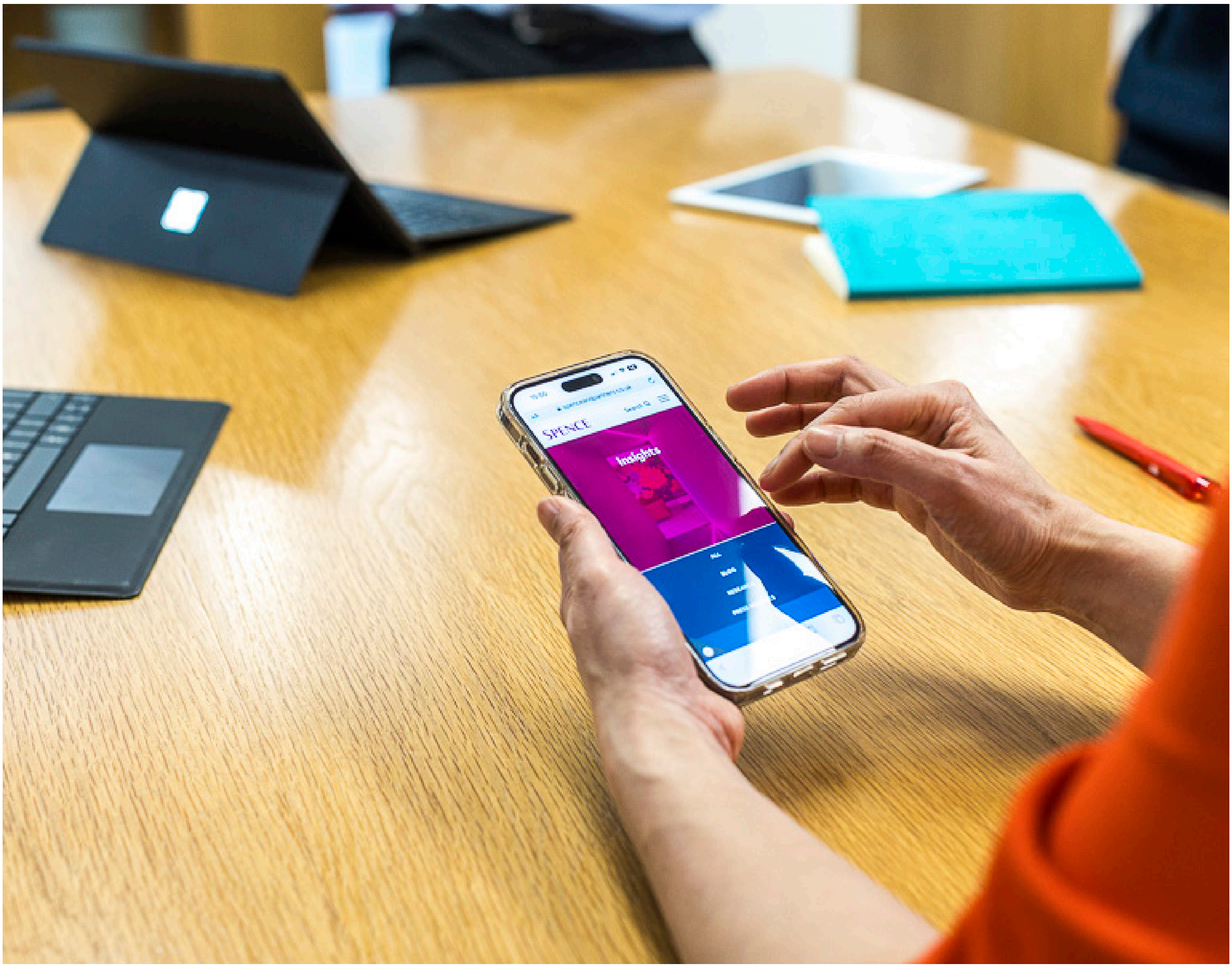
Summary of Control Objectives

This section provides summary information and assurance on the design, description and operation of the control procedures for the administration, accounting and information technology functions, as described in the Directors' report for Spence & Partners.

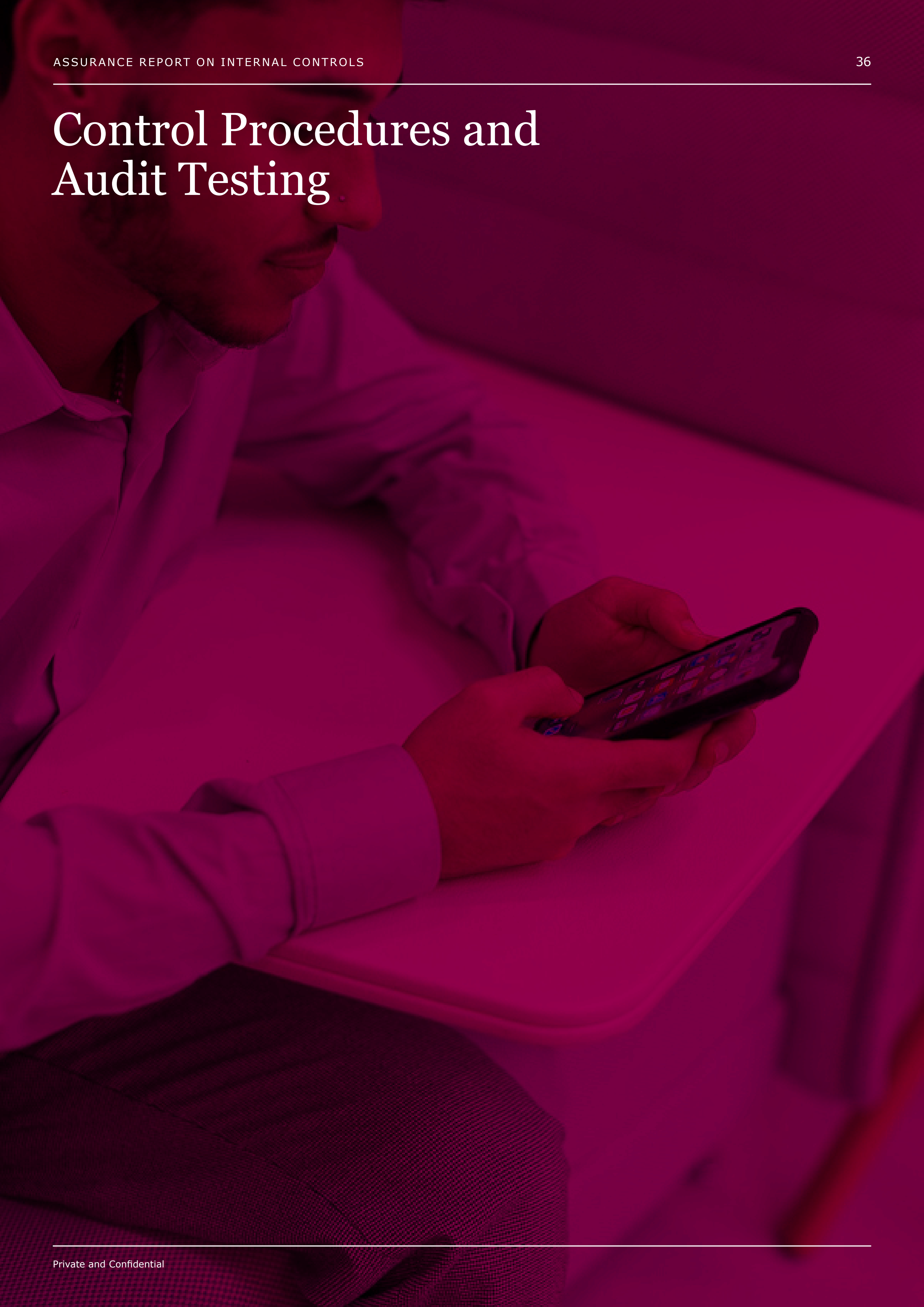
Control Objective	Audit Finding
1. Accepting Clients	
Accounts are set up and administered in accordance with client agreements and applicable regulations.	**No exceptions noted.**
Complete and authorised client agreements are operative prior to initialising administration activity.	**No exceptions noted.**
Pension schemes taken on are properly established in the system in accordance with the scheme rules and individual elections.	**No exceptions noted.**
2. Authorising and Processing Transactions	
Contributions to defined contribution plans, defined benefit schemes, or both, and transfers of members' funds between investment options, are processed accurately and in a timely manner.	**No exceptions noted.**
Benefits payable, and transfer values, are calculated in accordance with scheme rules and relevant legislation and are paid on a timely basis.	**No exceptions noted.**
3. Maintaining Financial and other Records	
Member records consist of up to date and accurate information, and are updated and reconciled regularly.	**No exceptions noted.**
Contributions and benefit payments are completely and accurately recorded in the proper period.	**No exceptions noted.**
Investment transactions, balances and related income are completely and accurately recorded in the proper period.	**No exceptions noted.**
Scheme documents are complete, up to date and securely held.	**No exceptions noted.**
4. Safeguarding Assets	
Member and scheme data is stored appropriately to ensure security and protection from unauthorised use.	**No exceptions noted.**
Cash is safeguarded and payments are suitably authorised and controlled.	**No exceptions noted.**
5. Monitoring Compliance	
Contributions are received in accordance with the scheme rules and relevant legislation.	**No exceptions noted.**
Services provided to pension schemes are in line with service level agreements.	**No exceptions noted.**
Transaction errors are rectified promptly, and clients treated fairly.	**No exceptions noted.**

Control Objective	Audit Finding
6. Reporting to Clients	
Periodic reports to participants and scheme sponsors are accurate and complete, and provided within required timescales.	**No exceptions noted.**
Annual reports and accounts are prepared in accordance with applicable law and regulations.	**No exceptions noted.**
Regulatory reports are made if necessary.	**No exceptions noted.**
7. Restricting access to systems and data	
Physical access to systems is restricted to authorised individuals.	**No exceptions noted.**
Logical access to In-scope systems and data is restricted to authorised individuals in accordance with job roles and/or business requirements.	**No exceptions noted.**
Client and third-party access to In-scope systems and data is restricted and/or monitored.	**No exceptions noted.**
Segregation of incompatible duties within, and across, business and technology functions is formally defined, implemented, updated and enforced by logical security controls.	**No exceptions noted.**
8. Maintaining integrity of the systems	
Scheduling and internal processing of data is complete, accurate and within agreed timescales.	**No exceptions noted.**
Transmission of data to/from external parties is complete, accurate, executed within agreed timescales and secure in line with external party agreements.	**No exceptions noted.**
Network perimeter security devices are installed and changes are tested and approved.	**No exceptions noted.**
Anti-virus definitions are periodically updated across all terminals and servers, deployment and Settings are periodically reviewed and updated when required, and patterns of attempted external breaches are monitored.	**No exceptions noted.**
Data received from external parties is scanned for known vulnerabilities, any compromised data is quarantined and definitions of threats are periodically updated.	**No exceptions noted.**
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.	**No exceptions noted.**
Data migration or modification is authorised, tested and, once performed, reconciled back to the source data.	**No exceptions noted.**
Changes to existing In-scope systems, including hardware upgrades, software patches and direct configuration changes, are authorised, tested and approved in line with policy.	**No exceptions noted.**

Control Objective	Audit Finding
10. Recovering from processing interruptions	
IT related Disaster Recovery Plans are documented, updated, approved and tested.	**No exceptions noted.**
In-scope systems and data are backed up and tested such that they can be restored completely and within agreed timescales.	**No exceptions noted.**
Problems and incidents relating to In-scope systems are identified and resolved within agreed timescales.	**No exceptions noted.**
Performance and capacity of In-scope systems are monitored and issues are resolved.	**No exceptions noted.**
The physical IT equipment is maintained in a controlled environment.	**No exceptions noted.**
11. The physical IT equipment is maintained in a controlled environment.	
Outsourced activities provided by Subservice Organisations are governed by contracts and service level agreements that are authorised and subject to regular review.	**No exceptions noted.**
The services provided by Subservice Organisations are regularly monitored and assessed against the standards set out in the service level agreements.	**No exceptions noted.**



Control Procedures and Audit Testing



Control Procedures and Audit Testing

This section provides summary information and assurance on the design, description and operation of the control procedures for the administration, accounting and information technology functions, as described in the Directors' report for Spence & Partners.

Control Objectives	Audit Finding
1. Accepting Clients	
On confirmation that Spence is prepared to act, a Fee & Service Agreement is issued for signature on behalf of the trustees. The Agreement reflects the services Spence is being contracted to provide and the agreed method of charging. As part of the client take-on process, the relevant client take-on documentation is completed, as outlined in the client take-on process note. Standard administration tasks are also added to the workflow system, reflecting standard performance timescales, or bespoke timescales, as may be detailed in the Fee & Service Agreement.	Verified for a sample of new schemes during 2022 that Fee & Service Agreements were in place and signed by both Spence and the relevant scheme trustee. Confirmed for each of the sampled schemes that the Agreement reflects the services Spence have been contracted to provide and the agreed method of charging. Verified for the sample of new scheme acceptances during 2022, that the Client Initial Take On Document, Pre-Appointment Conflict Consideration and Accepting Business Risk Management were completed and signed off by the Spence client manager. For the sampled schemes, confirmed that the standard administration tasks have been added to the workflow system in line with the timescales as detailed in the Agreement. **No exceptions noted.**
As part of the implementation process a copy of all scheme documentation is requested. This documentation is reviewed, and where administration services are provided, forms the basis of scheme benefit specifications. Where appropriate, the Benefit Specification is reviewed and signed off by the trustees and/or the scheme's legal advisers, particularly if there is any ambiguity in interpretation, or if there is any concern that the benefits provided do not comply with legislative requirements. Data is requested in all forms and any electronic data is imported onto Spence administration systems and tested against the data quality standards set out by The Pensions Regulator. Membership statistics are reconciled to the last set of audited Accounts and to control totals provided by the previous administrator. Where necessary, remedial action is proposed in the event that data is materially deficient to the extent that Spence cannot carry out some or all of the services it have been contracted to perform. The pension database team is responsible for data migration projects. A scheme installation checklist is completed which follows the key stages of the migration. Logs are maintained of all issues along with details of their resolution. The results of sample data checks and the reconciliation are reviewed by the pension database team manager to ensure procedures have been followed.	Confirmed for a sample of new schemes that a copy of scheme documentation was requested, subsequently reviewed, and formed the basis of benefit specifications. Confirmed for the same sample of new schemes that a Benefit Specification was signed by the trustee and where applicable by the scheme's legal advisers. Verified for the sample that the Scheme Installation Checklist has been signed off, data was imported into the administration system, Mantle, and reconciled. **No exceptions noted.**

Control Objectives	Audit Finding
On confirmation that Spence is to be appointed, a Fee & Service Agreement is issued for signature on behalf of the trustees and, except in exceptional circumstances, work should not commence until a signed Agreement is in place. The Agreement will be based on a Spence template agreement, suitably amended to reflect the services Spence is being contracted to provide and the agreed method of charging. Production of the Fee & Service Agreement is carried out centrally to ensure appropriate control over the template to be used and, also, maintenance of a central record of all Agreements issued. Similarly, any amendments to the template agreement can only be made by certain individuals.	Confirmed for the sample of schemes that the Agreement was signed prior to work on the scheme commencing. Confirmed that the Fee & Service Agreements were based on the Spence template agreement and had been altered for the specific services being provided. **No exceptions noted.**
Wherever possible, Spence requests sight of any previous administrators' specifications and/or details of custom and practice to establish any precedent in areas of interpretation of the Rules where this might not be clear and where member specific benefits may override, for example where senior employees have an entitlement to different benefits, detailed in an individual announcement letter.	Verified that requests to view any previous administrator's specifications were made during 2022 where necessary. **No exceptions noted.**
The Benefit Specification is prepared by the administrator and reviewed by the client manager. Where appropriate the Benefit Specification is reviewed and signed off by the trustees and/or the scheme's legal advisers, particularly if there is any ambiguity in interpretation or if there is any concern that the benefits provided do not comply with legislative requirements.	Verified for the sample of new schemes during 2022 that the benefit specification was signed by the trustee and the legal advisor where applicable. **No exceptions noted.**
All documentation is scanned, tagged and filed in SharePoint, for ease of reference.	Verified for a sample of five new client take ons during 2022, that documentation is scanned and saved in SharePoint with the originals held in secure storage. **No exceptions noted.**
2. Authorising and processing transactions procedure	
Procedures are followed for banking cheques and electronic credits and contributions monitoring whereby all cheques received are logged and banked within 24 hours, or as soon as practicable after that, taking into account weekends, bank holidays or staffing levels. Electronic credits are logged by the accounts team. The paperwork accompanying the cheque/ electronic credit is passed to the accounts team which prepares a deposit form and updates the transaction on Xero to record receipt of the contributions. Electronic credits are exported daily, and deposit forms are completed on Mantle/Xero/Quickbooks. Deposits are then reviewed and filed on the system. Cheque credits are scanned upon receipt and sent to treasury. Scanned cheques are then uploaded to deposit for backing.	Verified for a sample of receipts and cheques received throughout 2022 that they were logged and banked within 0 to 5 business days. Confirmed that electronic credits are exported daily with deposit forms completed on Mantle and Xero updated where appropriate. Confirmed for a sample of cheques, that they were scanned upon receipt by the Business Support Team and forwarded to the treasury department prior to being uploaded. **No exceptions noted.**

Control Objectives	Audit Finding
The contributions monitoring spreadsheet is reviewed on the 19th of each month and any outstanding contributions usually received by that date are followed up. The receipt of the remainder is monitored. Any late contributions are notified to the client manager, actuary and trustees. They are recorded on the breaches log, which is on the agenda at the quarterly Board meetings	Confirmed that the contributions monitoring spreadsheet is reviewed on the 19th of each month, with it used to reconcile the contributions to the schedule of contributions for all schemes. Verified for a sample of contributions that they were processed accurately and on a timely basis, and our testing did not identify any late contributions. Confirmed that any breaches are notified to the client manager, scheme actuary and administration manager as appropriate, and recorded on the breaches log. Verified through review of the February, June, and October 2022 Board minutes, that any breaches are reported to the Board as part of the Risk and Audit Report. **No exceptions noted.**
At least three months in advance of a member's normal retirement age a task is created on the workflow system. An administrator can be notified of a task to calculate benefits by post, email or 'other' e.g. phone call, verbally, meeting minute. The request is set up as a task within the workflow system and an administrator completes the appropriate checklist.	Verified for a sample of members, that a task was created on the workflow at least three months in advance of their normal retirement age. Confirmed for the sample of members, that the benefits calculation was sent via post which is the default method for issue of calculations. Verified for our sample, that the members were sent their benefits calculations and the administrator completed the appropriate checklist. **No exceptions noted.**
Calculations are processed in accordance with the scheme benefits specification, which is produced in line with the scheme rules. All calculations are checked by a senior administrator or administration manager. Approval workflows are run against all calculations and documents prepared, along with the checklist. All transfer value calculations are completed by Mantle (where set up on this basis) and checked by the Actuarial team in line with set thresholds which may differ from client to client. The workflow tasks are monitored by the administrator and the administration manager with the aim that they will be finalised within the service level agreement agreed with the client. Once the task is finalised, the workflow checklist will be completed. Payments are processed by the treasury team following the request and with the appropriate backing papers detailing the amount payable. Payment withdrawal forms are processed and checked by separate staff and cheques/electronic payment instructions are signed in accordance with the bank mandate by staff that are different from the processor and checker. Once a task has been completed it is closed off on the system.	Verified for a sample of scheme calculations that they were processed in accordance with the scheme rules, signed off as reviewed, that the actuarial calculation was completed by Mantle and that the workflow checklist was completed within the service level agreement agreed with the client. **No exceptions noted.** Verified for a sample of payments that they were processed accurately and on a timely basis after the initial request. All calculations were approved, the checklist prepared and approved for electronic payments, two relevant signatories completed on all cheques and the account balance updated. For the sample, it was confirmed that the payments were requested, processed and confirmed by three different individuals. **No exceptions noted.**

Control Objectives	Audit Finding
Every month a payroll administrator updates the control spreadsheet with the payment date and the latest date on which the payment file can be submitted to the bank (taking into account bank/public holidays). The payroll administrator maintains a monthly payroll checklist, detailing for each payroll, each stage of running and paying the payroll. This checklist is monitored during the period to ensure payment dates are met.	Confirmed for a sample of periods that the control spreadsheet is updated with the payment date and the cut-off date for submission to the bank. Verified for the sample of periods that the payroll checklist has been prepared, maintained and monitored to ensure payment dates are met. **No exceptions noted.**
Any changes are notified to the payroll team by a set monthly cut-off date and are applied to the payroll. As changes are received, they are added to the carry forward spreadsheet. The payroll is run using Spence's in-house software, Mantle and is reconciled by the payroll administrator for recorded changes against the previous payroll run. Each reconciliation is peer reviewed for accuracy.	Verified for a sample of periods that changes have been notified to payroll by the cut-off date, applied to the payroll and added to the carry forward spreadsheet as they have been received. Confirmed that the payroll is run using Spence's in-house software, Mantle. Verified for the sample of monthly payrolls that reconciliations of the payroll file against payroll data have been undertaken and that all payrolls have been peer reviewed and approved for payment. **No exceptions noted.**
Reconciliations and payroll reports for each period are saved on our file management system, SharePoint or Mantle. The payment file is checked against the payroll data before being uploaded to the online banking facility.	Verified that reconciliations and payroll reports for a sample of periods are saved in Mantle. Verified for a sample of monthly payrolls that the payroll file was checked by the payroll administrator against the payroll data prior to upload to the online banking facility. **No exceptions noted.**
Monthly payrolls are checked and approved for payment by the administrator. The administrator will reconcile any changes to the payroll against the administration data to check that the correct pensions are being paid. Pension increases are initially calculated in accordance with the scheme rules. Recurring tasks are then set up on the workflow system for the increases to be calculated, either on anniversary or annually, depending on the scheme rules. The increases are checked by a senior administrator and a checklist is completed.	Verified for a sample of monthly payrolls that they are checked and approved prior to payment being made. Reviewed evidence of the administrator reconciliation of changes to the payroll against administration data for a sample of periods and verified the accurate pension payments were made. Verified for a sample of monthly payrolls that pension increases have been calculated in line with scheme rules and a recurring task set up for future increases to be calculated. Verified that pension increases have been checked by a senior administrator and a checklist completed. **No exceptions noted.**

Control Objectives	Audit Finding
3. Maintaining financial and other records	
For schemes that have active members, a recurring task is set up on the workflow system for pre renewal schedules to be sent to each client site prior to the renewal date. A checklist is updated throughout the process. Once all the data has been returned, the administrator follows the annual renewal checklist and updates members' salary and status data, which is reconciled against the data received from the client. Any discrepancies are investigated and resolved by the client management team. The renewal is then processed and benefit statements for each active member are produced. All calculations and statements are checked by a senior administrator.	Identified one instance within our sample testing of schemes with active members where a workflow system for pre renewal schedules to be sent was not in place and a checklist was not updated throughout the process. We did however note that this did not affect the distribution of statements to members on a timely basis, and was an instance of non-compliance with internal process ie completion of a checklist. Confirmed that the renewals were processed, with calculations and the benefit statements peer reviewed by a senior administrator. **No exceptions noted.**
Following any change in status, member data is also kept up to date through periodic and ad-hoc data loads including payroll data, pension increase data and changes to personal details. The information relating to these data loads is provided to the pension administration team. On receipt of data, a business analyst follows the scheme update checklist to load the data onto Mantle. The data is reconciled back to the source data. Copies of work relating to data loads are held on our document management system.	Verified for a sample of data loads and periodic updates of member data that the checklist has been completed, data reconciled back to source, the updates have been peer reviewed and information relating to the change is held on Mantle. Verified for the sample that the scheme update checklist is completed by a business analyst and the information is uploaded to Mantle. **No exceptions noted.**
Any changes to the scheme membership are recorded on Mantle when advised by members or clients or trustees. When calls are received from members, verification is sought by asking for date of birth and National Insurance number.	Verified for a sample of deaths, transfers, retirements and data changes that following the receipt of all relevant information, the checklist/workflow is updated in Mantle, calculations completed, peer review is undertaken, and the relevant letter sent to the client confirming all processed in a timely manner. **No exceptions noted.**
All changes are checked by another administrator. Following the change in the member's status it is updated on Mantle. A workflow checklist is completed and checked by a senior administrator.	Verified for a sample of deaths, transfers, retirements and data changes that the changes were checked by another administrator, Mantle had been updated and the workflow checklist had been completed and checked by a senior administrator. **No exceptions noted.**
Movements in active, deferred and pensioner numbers are reconciled on an annual basis as part of the accounts preparation process. Any discrepancies are investigated and resolved.	Verified for a sample of schemes that an annual report on membership is prepared with member numbers reconciliation included in the scheme accounts. Our testing did not identify any discrepancies. **No exceptions noted.**

Control Objectives	Audit Finding
Receipt of any documentation from members or third parties is scanned and filed in SharePoint and/or Mantle and checked by the administrator. Documentation for transfers out includes the discharge forms (CETV CO, CETV Enhanced CO, CETV Enhanced FS & MP CI) signed by the member, and details of the receiving scheme and for deaths and retirements includes birth/ death/ marriage certificates, retained benefit forms and evidence, signed option forms and trustee or company authorisation where required. Copies of documents are tagged and filed in SharePoint/Mantle. Any original documents are returned to the member by recorded delivery.	Confirmed for a sample of transfers out, deaths and retirements that signed scheme documentation is retained on SharePoint, all requested scheme information was made available and reviewed electronically on either SharePoint or Mantle systems. Verified that original documents are returned to members by way of recorded delivery and postage receipts are retained to evidence return. **No exceptions noted.**
The pension payroll administrator is advised of any new pensions to be added to the payroll and this request is checked by another administrator. The cessation of a pension on, for example, a pensioner death is advised to the pension payroll administrator immediately by the scheme administrator.	Verified for a sample of new pensions that the procedure is in place with checklists and calculations completed and manager review is undertaken for new pensions added to the payroll. Verified for a sample of members in relation to pensioner deaths that the pension payroll administrator was advised immediately with appropriate action taken. **No exceptions noted.**
Each scheme has its own bank account, and the financial records are maintained separately. Biometric readers / passwords are required to access each scheme account. All credits and payments are recorded on a scheme cashbook following the procedures for banking cheques and electronic credits, and the procedures for making cheques and electronic payments from the scheme bank account.	Confirmed, for a sample of schemes that each had their own bank account. Confirmed through observation that access to each scheme account is limited to those staff members who work on each specific scheme. These staff members have their own unique log-in and access is controlled by the IT department. Verified for the same sample of scheme bank accounts that monthly reconciliations between the cashbook and the bank statement are undertaken within seven days from the end of the month, with appropriate segregation of duties and peer review procedures in place. **No exceptions noted.**

Control Objectives	Audit Finding
The scheme deposit form is filed along with any supporting documentation and the amount received is checked against any schedule/confirmation advice. The scheme withdrawal form is checked against, and filed along with, the supporting benefit documentation. The procedures for carrying out bank reconciliations are followed, whereby the cashbook is reconciled against the bank statement for the trust account each month/quarter and any anomalies are investigated. Bank reconciliations are completed within the next working month of receipt of the bank statement unless queries arise which causes a delay. Un-cashed cheques are monitored by the treasury team and if more than one month old are notified to the scheme administrator.	Verified for a sample of scheme deposits, they were checked for accuracy and filed against supporting documentation. Confirmed for a sample of schemes that bank reconciliations between the cashbook and the bank statement are completed on a monthly basis. Ensured through review of sign off evidence that the sample of bank reconciliations are checked by the Fund Accountant and are noted within the system as reconciled when complete. Our sample of bank reconciliations did not identify any instances where anomalies existed that required investigation. Confirmed, by way of review for a sample of days, that a deposit report is run from the system on a daily basis showing all cheque deposits. This is reviewed by the Treasury team and any uncashed cheques are queried with the administration team. **No exceptions noted.**
The cheque system is reviewed, and any outstanding lodgements are processed or queried and cleared down. Bank statements and the bank reconciliation reports are filed on SharePoint/Xero and the paper copies of bank statements are filed with the other post items, but in a separate folder.	Confirmed, by way of review, that a deposit report is run from the system on a daily basis showing all cheque deposits. This is reviewed by the Treasury team and any unidentified cheques are queried with the administration team. Confirmed that cheques are rarely received, for any cheques that are received it is highly likely that staff will be aware of its arrival, and it will be cashed as soon as possible. Verified for a sample of receipts and cheques received throughout 2022 that they were logged and banked within 0 to 5 business days. It has been verified that bank statements and bank reconciliation reports are filed on the Mantle Hosting platform. Verified that all bank statements are now downloaded rather than sent by the bank and that reconciliations are completed digitally. **No exceptions noted.**
As part of the annual scheme accounting process the fund accountant reconciles the contributions to the schedule of contributions and benefit payments to the member movement report produced from Mantle. Any discrepancies are investigated and resolved.	Verified that a sample of contributions were reconciled to the schedule of contributions and benefit payments to the member movement report. Confirmed that any discrepancies were investigated and resolved. **No exceptions noted.**

Control Objectives	Audit Finding
As part of the annual accounting process, the fund accountant reconciles the investment valuation, investment income, purchases and sales with data received from the investment managers. Any discrepancies are checked and investigated by the fund accountant. Investments and disinvestments in the scheme cashbook are reconciled to the investment managers' transactions.	Verified for a sample of schemes that investment valuation, investment income, purchases and sales in the scheme cashbook were reconciled to the investment managers record of transactions by the fund accountant. Confirmed that any discrepancies had been investigated by the fund accountant. **No exceptions noted.**
Journals are posted to the trial balance and period end balances inserted into the accounts template on an annual basis, in accordance with the Statement of Recommended Practice ("SORP") and disclosure regulations.	Verified for a sample of schemes that a standard reporting format was in place for the creation of the annual report and accounts. The Statement of Recommended Practice (SORP) was used as the template to prepare the scheme annual report and accounts. Confirmed that period end balances are detailed within. Confirmed that once the accounts were in draft format, they were reviewed by another fund accountant to ensure they were in line with the requirements of SORP. Confirmed for a sample of months, that monthly meetings were held for monitoring purposes. **No exceptions noted.**
No original documents are held on file but are sent to the legal advisers, trustees, or offsite storage. All scheme documents are scanned and filed in SharePoint. Scheme documents are obtained and filed on client take on. Any new or amending documentation is scanned and filed to ensure that the latest scheme documentation is maintained and held on file.	Verified through our testing that all scheme documentation is scanned and saved in Mantle/ SharePoint with the originals held in secure storage or sent on to the offsite storage provider, Doxbond. Confirmed through a walkthrough of the Belfast office that any original documentation is stored in a storage room with controlled access through biometric authentication for authorised individuals. **No exceptions noted.**
4. Safegaurding Assets	
Access to Spence's premises is restricted to authorised personnel. Additional restrictions are in place in respect of access to IT areas.	Obtained the Physical and Environmental Security process document (Version 21, dated 01/09/22) and confirmed that it is subject to review on an annual basis and clearly outlines the physical security controls for access to all office locations. Verified through a walkthrough of the Belfast office that a key fob is required to access both the main building and lift to the office floors. Verified through the same walkthrough that both a key fob and physical key are required to access the two server rooms.

Control Objectives	Audit Finding
	Confirmed through review of the server room list of key holders that only staff listed are authorised to access the Server rooms. Authorised staff gain access with permissioned key fobs, where access permissions are controlled by the IT department. **No exceptions noted.**
Passwords are used by individual members of staff and laptops/PCs are locked when staff are away from their desks. Only the IT team can set up access to systems and access to scheme data on Mantle.	Inspected the Access Control Policy and confirmed that password security requirements are set out and aligned to the actual settings configured in the domain's account policies. These requirements include a threshold to lock laptops/PC when staff is away from desks. Verified that a clear desk policy is in place and clearly outlined within the Business Support and Office Management Processes (version 22, dated 31/08/2022). The policy is subject to review on an annual basis and is communicated to all staff. Confirmed that only the IT team can set up access to systems and access to schema data on Mantle. **No exceptions noted.**
All new staff complete an online data protection training course incorporating GDPR as part of their induction when they join the Company. Mandatory biennial training is delivered with refresher training given periodically, as and when required. Staff sign a security and confidentiality policy, a copy of which is held on their personnel record.	Verified for a sample of new joiners in 2022 that an Access NI check was completed, a non-disclosure agreement and Security and Confidentiality policy had been signed and retained on file within the first two weeks of their employment. Verified for the sample of new joiners that mandatory training was completed across the following areas; Conflicts of Interest, GDPR, Anti-Bribery, Anti-Money laundering and Information Security. This list is not exhaustive and refresher training is provided every two years. **No exceptions noted.**
Member and scheme data is stored electronically on Mantle or in SharePoint. Any data/correspondence held in paper form pre-dating the introduction of SharePoint is securely held offsite. Spence outsources its off-site storage and archive facilities to a specialist organisation, Doxbond. In the event that it is necessary to retrieve paper files, these are scanned to the system and the originals returned to off-site storage.	Verified through a walkthrough of the Belfast office that all mail (which may include member or scheme data) is securely stored in locked filing cabinets in the filing room which has restricted access and requires biometric authentication completion by authorised individuals. Verified that all scheme documentation is scanned on Mantle/SharePoint and all archived documents are stored securely off site with the secured storage provider, Doxbond. All documentation collected by Doxbond is recorded on a receipt and is signed by both Spence and Doxbond. The same applies to any documents recalled by Spence. All information relating to archived material is updated and maintained on a master spreadsheet by a member of the Business Support team. **No exceptions noted.**

Control Objectives	Audit Finding
All incoming correspondence is scanned by the business support team. Outgoing mail is created and filed on SharePoint or Mantle. No paper is retained in the work area and any printed material from the system is securely destroyed. All hard copies of correspondence are retained and stored in Doxbond.	Confirmed through testing a sample of deaths, transfers out and retirements, that correspondence from members is scanned by the business support team and stored against their member file in Mantle/SharePoint. Similarly, for the same sample we confirmed that all correspondence from Spence to the members was also stored against the members' file in Mantle/SharePoint. Verified that a clear desk policy is in place and clearly outlined within the Business Support and Office Management Processes (version 24, dated 31/08/2022). The policy is subject to review on an annual basis and is communicated to all staff. Confirmed through a walkthrough of the Belfast office that desks not in use were clear of documentation. Confirmed that confidential waste bins are located in the office to securely dispose of sensitive information. Spence are issued with certificates of destruction upon collection and destruction of the bin contents. The majority of paper documentation is securely stored off site and is managed by Doxbond. All documentation collected by Doxbond is recorded on a receipt and is signed by both Spence and Doxbond. The same applies to any documents recalled by Spence Confirmed, via the walkthrough, that all sensitive paper documentation on site is securely located within the filing rooms which are only accessible by authorised staff with biometric keypad access. **No exceptions noted.**
Spence has obtained ISO27001 (information security) accreditation.	Confirmed that Spence had obtained the ISO27001 (information security) accreditation certificate which is also published on the Spence company website. **No exceptions noted.**
When taking on the administration of the trust account, bank forms and required information are sent to the bank along with a copy of the trust deed. The Bank is notified of a change in authorised signatories and appropriate documentation is forwarded to the bank.	Verified for a sample of new schemes with bank accounts opened during 2022, that bank forms and mandates were completed, signed by the trustees, and signed by authorised signatories prior to forwarding to the bank along with a copy of the trust deed. **No exceptions noted.**
Cheques received are logged and banked within 24 hours, or as soon as practicable after that, taking into account weekends, bank holidays or staffing levels affected due to the COVID-19 pandemic. Payments are processed in accordance with instructions. Cash movements are recorded on a daily basis on the internal accounting system.	Verified as part of testing for Section 2, Authorising and Processing Transactions. **No exceptions noted.**

Control Objectives	Audit Finding
Trust account balances are circulated to the administration team and any of the client managers who have requested bi-monthly updates (approximately on 1st and 19th day of each month). Payments are, processed and checked by separate individuals. At least two authorised signatories are required for all payments and are different from the requester, processor, and checker.	Confirmed for a sample of months that trust account balances are circulated to the administration team and client managers who have requested updates, on a bi-monthly basis. Payments verified as part of testing for Section 2, Authorising and Processing Transactions. **No exceptions noted.**
Cheque books are held in a secure location only accessible by designated staff.	It was verified via a walkthrough of the Belfast office, that cheque books are securely stored within the Treasury department filing cabinet within the filing room in the office. Verified that the filing room is only accessible to authorised staff via a biometric scanner and only members of the Treasury department have access to keys for the Treasury filing cabinet. **No exceptions noted.**
Cashflows are carried out in accordance with the Cashflow Procedures and investment, or disinvestments are carried out where appropriate. The cashflow administrator ensures that the investment manager processes the investment/disinvestment and the disinvestment amount requested is received into the scheme bank account.	Verified for a sample of schemes that the scheme cashflow is carried out monthly or quarterly by the cash flow administrator, as determined by the size of the scheme, peer reviewed and client manager reviewed, and the investment or disinvestment transaction confirmed. **No exceptions noted.**
Scheme expenses are only authorised with appropriate approval on the invoice, by email or on SharePoint. The cashflow administrator also needs to be aware of the payment.	Confirmed for a sample of scheme expenses during 2022, appropriate authorisation was completed prior to issue of payment. Verified for a sample of invoices, that they are approved, and an email is retained on the system from the authoriser and attached to the payment information. Confirmed, in each instance that the cashflow administrator had been made aware of the payment. **No exceptions noted.**
5. Monitoring Compliance	
The procedures for contributions monitoring are followed. The credit is logged and at the same time processed on the accounting system. Cheques are banked within 24 hours, or as soon as practicable after that taking into account weekends, bank holidays or staffing levels affected due to the COVID-19 pandemic. A scanned copy of the latest Schedule of Contributions is held on SharePoint.	Verified that a sample of contributions were processed accurately and on a timely basis and outstanding contributions were followed up. Verified that an up-to-date Schedule of Contributions for a sample of schemes are held on SharePoint. **No exceptions noted.**

Control Objectives	Audit Finding
The amounts due are entered on the contributions monitoring spreadsheet and monitored. Any unusual differences are investigated. The contributions monitoring spreadsheet is reviewed on 19th of each month and any outstanding contributions usually received by that date are followed up. The receipt of the remainder is monitored. Any late contributions are notified to the client manager, actuary, and trustees. They are recorded on the breaches log which is on the agenda at the quarterly Board meetings.	Verified that the amounts due are entered on the contributions monitoring spreadsheet, which is reviewed on the 19th of each month by the fund accountant. Confirmed that late payment of contributions is recorded in the Incident Management Application. Verified for a sample of errors that the appropriate notifications have been made to the administration manager, client manager and scheme actuary as appropriate. Confirmed through review of the February, June and October 2022 Board minutes, that any breaches are reported to the Board as part of the Risk and Audit Report. Confirmed that presentation of the Report is a standing item on the agenda for quarterly Board meetings. **No exceptions noted.**
Service Level Agreements (SLAs) are agreed with the trustees and the administration team aim to carry out services and tasks accurately and efficiently, and to meet SLAs.	Verified that for a sample of schemes, agreed SLAs are in place. Verified for a sample of schemes that performance against the SLAs have been reported to the trustees in the format of administration reports. **No exceptions noted.**
A workflow system is in place for all tasks carried out by the administration team. As soon as a task is initiated it is recorded on the workflow system by the administrator (the owner). Each task has a SLA that is clearly defined from when the task begins and when it ends.	Verified through a walkthrough on screen, that workflows in the Mantle system include tasks to be carried out by the administration team, the date on which the task was initiated, the deadline for completion of the task, how many days remain until the completion deadline and the status of the workflow (i.e. ongoing, completed or overdue). **No exceptions noted.**
Reports can be run off the workflow system so that SLAs and statutory deadlines can be monitored. The administrator, and the administration manager, monitor each task against the service standards and disclosure deadlines so as to highlight any instances where service standards are being breached. Service standards are always shorter than disclosure deadlines and, therefore, disclosure breaches should be avoided unless extenuating circumstances arise. The contents and frequency of administration reports are agreed by the scheme trustees. They will contain a report from the workflow system detailing the tasks undertaken during the relevant period and whether the SLAs have been met. This allows the trustees to monitor the administrators' performance.	Verified through walkthrough of the workflow system that the internal deadlines have been set shorter than the statutory disclosure deadlines and therefore disclosure breaches should be avoided. Confirmed through review that workflows in the Mantle system detail the number of days taken to complete the task and the status of the workflow (i.e., ongoing, completed, or overdue). Confirmed that there were not any instances in our sample where extenuating circumstances caused a delay in completing a task in the workflow system. Verified for a sample of schemes that quarterly Administration reports contain a report from the workflow system detailing the tasks undertaken in the period and whether the SLAs have been met. **No exceptions noted.**

Control Objectives	Audit Finding
Procedures are followed for errors & omissions, whereby any transaction errors are notified immediately by the administrator to their line manager and the client manager. Details of the error or omission are entered in the appropriate section in the 'Regulatory Breaches Log' and consideration is given to the need for any further action that may be required. All errors and omissions are notified to the Board as part of the internal management information reporting process. The client manager will determine if any further action is required and notify the relevant parties to implement.	Confirmed through review that the Incident Management Application has been used for the recording of all incidents, omissions, regulatory and DPA breaches. Confirmed through review of a sample of errors, DPA breaches and regulatory breaches, they were appropriately recorded, with incident date, incident number, responsible party, incident details, the resolution outlined and where necessary, details of any future actions required. Reviewed minutes for the GRC and confirmed that incident reporting is a standing agenda item and the status of all incidents recorded are discussed. Reviewed the February, June and October 2022 Board minutes, and confirmed that errors, omissions and breaches are reported to the Board as part of the Risk and Audit Report. **No exceptions noted.**
6. Reporting to Clients	
A report of members reaching normal retirement date in the next 12 months is produced as part of the Stewardship Report. Any other movement requiring trustee approval is also recorded and detailed on the Stewardship Report. Stewardship Reports are provided for each scheme as determined by the trustees and client manager. The reports contain membership details provided from Mantle and a reconciliation of membership is carried out. They also contain details of any member movements for the period of the report. When the scheme administrator has checked the report, it is forwarded to the client manager for issue to the trustees, as and when required.	Verified for a sample of schemes that the quarterly stewardship reports were prepared and checked by a supervisor to confirm the completeness and accuracy of member movements and reconciliations. Further confirmed that once checked by the scheme administrator, the reports were forwarded to the client manager for issue to the trustees as and when required. Verified for the sample of reports in 2022, that they contained a report of members reaching normal retirement date in the next 12 months and details of any member movements for the period of the report. **No exceptions noted.**
For schemes that have active members, a recurring task is set up on the workflow system for pre-renewal schedules to be sent to each client site prior to the renewal date. A checklist is updated throughout the process. Once all the data has been returned, the administrator follows the annual renewal checklist and updates members' salary and status data, which is reconciled against the data received from the client. Any discrepancies are investigated and resolved. The renewal is then processed and benefit statements for each active member are produced. All calculations and statements are checked by a senior administrator.	Verified as part of testing for Section 3. Maintaining Financial and Other Records. **No exceptions noted.**

Control Objectives	Audit Finding
Annual reports and accounts are prepared using the accounts template which complies with the latest SORP for pension schemes. Any changes to the standard template are logged on a proposed amendments spreadsheet. As part of the drafting process, annual reports are peer reviewed by another fund accountant in the team prior to audit. Evidence of peer review is maintained through SharePoint. A report and accounts project is set up to record completion of each task by the statutory deadline.	Verified for a sample of schemes that the Statement of Recommended Practice (SORP) template was used to prepare the scheme annual reports and accounts. Once the accounts were in draft format, they were reviewed by another fund accountant to ensure they were in line with the requirements of SORP. Confirmed for a sample of schemes that a project management workflow was established to record completion of each task by the statutory deadline. **No exceptions noted.**
The draft report will be passed to the client manager for review. Initially a timetable is set for signing within five months. Monthly meetings are scheduled to monitor progress of the report and accounts projects against the statutory deadlines. Following the meeting a report is circulated to the consultancy team, if requested.	Verified for a sample of scheme accounts that the accounts once in a draft format were reviewed by the client manager. Confirmed that an internal deadline of five months is set for the signing of scheme accounts against the statutory deadline of seven months. For a sample of accounts, confirmed that the accounts were signed within the five or seven month deadlines. Verified for a sample of months that monthly meetings occurred for the purpose of monitoring delivery versus the statutory deadline. **No exceptions noted.**
Procedures are followed for regulatory breaches which sets out the statutory deadlines applicable. The administrator, and the administration manager, monitor tasks on the workflow system to ensure that cases that are approaching the statutory deadline are highlighted and followed up. Where a case approaches the statutory deadline, the administrator informs the client manager. Any breach is notified by the administrator to the administration manager, the client manager and the scheme actuary as soon as he/she becomes aware of the breach. Details of any breach are entered in the relevant section of the 'Regulatory Breaches Log.	Confirmed that procedures are in place and outlined within the Incident Management process document in place (version 15, dated 17/01/2022) for the administrator and administrator manager to monitor tasks on the workflow system and corresponding statutory deadlines. Verified for a sample of five regulatory breaches that they were recorded in the Incident Management Application and Mantle system, and had been brought to the attention of the client manager and the scheme actuary. Confirmed through review of minutes for the GRC in 2022, that incident reporting (including breaches) is a standing agenda item and the status of all incidents recorded are discussed. **No exceptions noted.**
All compliance breaches are notified to the Board as part of the internal management information reporting process. The client manager/scheme actuary should determine if a regulatory report is required.	Reviewed the Spence February, June and October 2022 Board reports and packs, and confirmed that errors, omissions and breaches are reported to the Board. **No exceptions noted.**

Control Objectives	Audit Finding
7. Restricting access to systems and data	
The business operates across seven office sites, Belfast, Bristol, Glasgow, London, Manchester, Bristol and Birmingham. Physical and Environmental Process (11) outlines physical controls, securing offices, rooms, facilities, protecting against external and environmental threats, working in secure areas, public access, delivery and loading areas, equipment security, power supplies, cabling security, equipment maintenance, secure disposal or re-use of equipment, removal of property.	Verified that a key fob is required to access the building and lift to access the Belfast office floors. Confirmed through virtual walkthrough that staff access the Glasgow office using a key fob and staff access the Manchester office using a key card. London, Birmingham, Leeds and Bristol are serviced offices with a manned reception and access is controlled through passcards. Confirmed that a key fob and physical key are required to access the server rooms in the Belfast and Glasgow offices, whilst access to the Manchester server rooms is controlled through the restricted use of a physical key. Confirmed that the Birmingham, Bristol, London and Leeds office do not have server rooms. Reviewed the Physical and Environmental Process and confirmed that it outlines physical controls, securing offices, rooms, facilities, protecting against external and environmental threats, working in secure areas, public access, delivery and loading areas, equipment security, power supplies, cabling security, equipment maintenance, secure disposal or re-use of equipment, removal of property. **No exceptions noted.**
The primary IT infrastructure resides at a secure, ISO 27001 certified, world class, off-site data centre utilising Infrastructure as a Service (IaaS). Spence's full environment is replicated to a second Azure region (UK West). The building in which the Belfast office is located is manned by security during office hours and is locked outside office hours.	Confirmed that primary IT infrastructure is hosted at a secure ISO27001 certified off-site data centre utilising IaaS. This is hosted on two geographically separate data centres that are used to host the services to provide additional resilience. A replica of the primary data centre (UK South) is in place and is used in the event of disaster recovery (UK West). Observed within Microsoft Azure Recovery Services that the replication was noted to be healthy and protected with the last failover test performed during the audit period and no configuration issues were noted. Reviewed the Physical and Environmental Process and confirmed that it outlines physical controls, securing offices, rooms, facilities, protecting against external and environmental threats, working in secure areas, public access, delivery and loading areas, equipment security, power supplies, cabling security, equipment maintenance, secure disposal or re-use of equipment, removal of property. Verified that the Belfast office is manned by security at the security desk during office hours and requires authorised key fob access to enter the building. **No exceptions noted.**

Control Objectives	Audit Finding
Only staff who require access outside office hours are given keys as approved and issued by the Business Support team, which maintains a list of key holders. Opening and closing procedures for each location have been issued to all staff and awareness training has been conducted. A key fob is required for entry to the Glasgow office building, so is issued to all staff.	Verified that there is a key register in place which details the names of those in possession of keys to the office. Confirmed that staff in possession of keys are required to sign and date the register upon receipt of the keys and again once the keys have been returned. Confirmed that only emergency contacts are given keys for access outside office hours and emergency contacts are listed within the Physical and Environmental Security procedure document. Confirmed that opening and closing procedures for all offices have been issued to all staff. Confirmed through a virtual walkthrough of the Glasgow office that the main office and filing room is restricted to entry by a key fob. **No exceptions noted.**
Staff inform the Business Support team if keys or key fobs are lost. Access to the main office is restricted to entry by a key fob in Belfast and Glasgow, which is only provided to staff. Access to storage areas in the Belfast is restricted to staff using a biometric scanner and Glasgow offices is restricted to staff in possession of a key fob. Other authorised personnel (e.g. temporary staff and cleaners) are issued with key fobs providing access to the main office only, but not to restricted areas. Any visitors are recorded in the visitors' log and are issued with a pass, which contains their name, company, who they are visiting, and the time and date of entry. Passes are returned to reception on leaving.	Confirmed that the loss of a key fob must be reported to the Business Support Team. Lost key fobs are recorded on the key register and lost fobs are deactivated, and a new fob is assigned and activated. Verified through a walkthrough of the Belfast office that a key fob is required to access both the main building and lift to the office floors. Verified through the same walkthrough that the filing room in the Belfast office is restricted to staff using a biometric scanner. Confirmed through a virtual walkthrough of the Glasgow office that the main office and filing room is restricted to entry by a key fob and a register is maintained detailing the names of those in possession of key fobs. Verified that cleaners are provided with access to the building for the main office areas and are required to sign a non-Disclosure agreement on commencement of employment. Confirmed that visitors are required to sign in at reception prior to accessing the office and are provided with an office pass containing their name, company, who they are visiting, and the time and date of entry. Visitors are signed out by a member of the Business Support Team. **No exceptions noted.**
Windows laptops are configured by an automated build to have password protection and data encryption is enforced. Corporate Anti-Virus and Device Configuration policies for Windows, MacOS and Mobiles are managed via InTune. This enforces the same Security Baseline across the company.	For the sampled devices, confirmed that they are configured in InTune (Microsoft Endpoint Manager) and Microsoft Azure. These MDM solutions configured devices by an automated build to enforce settings aligned to the Security Baseline (i.e., password protection, data encryption, Corporate anti-virus and device configuration policies for Windows, MacOS and mobile devices) across the company assets. **No exceptions noted.**

Control Objectives	Audit Finding
The company enforces a clear desk and clear screen policy. This is enforced through the Security and Confidentiality Policy. Security Training and awareness sessions are run periodically for all staff. Any client correspondence or documentation containing client information left on any desk, or on the printers at the end of each day, is disposed of in the confidential waste. Individual staff members are accountable. A Governance, Risk and Compliance Focus Group manages all security weaknesses and vulnerabilities and meets quarterly and /or when required to review risks, vulnerabilities, treatment, corrective, and preventive plans. All security events / weaknesses are analysed for root cause, and business impact reviewed and issues escalated to Board for further action. Documentation is either stored electronically on the network or in paper form.	Verified there is a clear desk policy contained within the Physical and Environmental Security process document (Version 21, dated 01/09/22). Confirmed that a nightly sweep of each office is completed at the end of the working day to ensure all documentation has been secured. Confirmed that security training and awareness sessions are run periodically for all staff. Confirmed, during a walkthrough that confidential waste bins are located in each office location to securely dispose of sensitive information. For a sample of two quarters within 2022, confirmed via review of meeting minutes that the Governance, Risk and Compliance Focus Group met and reviewed the Incident Management application and updates were provided by representatives from each function within the business. **No exceptions noted.**
Documentation in paper form is stored off-site in secure storage facility with Doxbond (local to the Belfast office). When there is a need for paper documentation to be stored in the office it is kept in our secure storage areas in accordance with our clear desk policy.	Confirmed that the majority of paper documentation is securely stored off site and is managed by Doxbond. Confirmed for a sample of collections and retrievals over a sample of months in 2022 that a receipt is signed by both Doxbond and Spence when documents are collected from or retrieved by Spence or by Doxbond. Verified that there is a master spreadsheet which details all documentation that has been sent to Doxbond and the status of the documentation which is maintained by a member of the Business Support team. Verified via a walkthrough of the Belfast office that all sensitive paper documentation on site is securely located within the filing rooms which are only accessible to authorised staff through biometric keypad access. **No exceptions noted.**
As part of the Human Resources Security Process (Leavers Process 40) upon termination of employment, all access rights are disabled and any IT assets e.g. Laptop, mobile phone, keys, or fobs are returned, and codes are changed.	Verified for a sample of leavers that the IT checklist was completed on their last day, confirming that all access rights were disabled and any IT assets e.g. laptop, mobile phone, keys, or fobs were returned, and access codes changed. **No exceptions noted.**

Control Objectives	Audit Finding
All access to computer equipment and systems is protected by passwords. Passwords expire after 42 days, and users are prompted to change. The domain security policy requires that passwords must be complex, at least 14 characters in length, alpha numeric. This is detailed in the companies Security and Confidentiality Policy for staff and backed up by the Access Control Process (9). All data must be stored on the corporate network and data is only permitted to be stored locally on laptops that are corporate owned and registered within the MDM solution.	Observed the InTune and Microsoft Azure platform and confirmed that each operating system has a compliance policy that requires all access to computer equipment and systems to be protected by passwords. Confirmed that password settings on the domain are set to expire after 42 days, password complexity is enabled, with a minimum password length of 14 characters. Verified that password requirements set out in the Security and Confidentiality Policy are aligned to the configuration set in the domain security policy noted above. Confirmed that all data must be stored on the corporate network and data is only permitted to be stored locally on laptops. Observed the InTune (Microsoft Endpoint Manager admin centre) and Microsoft Azure and managed by these MDM solutions. The devices are regularly checked for compliance to the relevant operating system policies. **No exceptions noted.**
Access to data stored on the network is restricted using appropriate permissions. Functional groups of users are maintained, each with appropriate levels of access permissions. Only authorised IT Team colleagues can amend an individual’s permissions outside of SharePoint Team access. Otherwise team owners can authorise access to SharePoint sites. Access rights are reviewed and amended as necessary i.e. when roles change or new members of staff join the company. Details of the restrictions in place on the network are documented. Most of the application software used is not restricted to authorised individuals, however, some applications that are specific to a job function, for example, cash management, pension administration, etc., are restricted to only those who have the associated privilege. User access is approved by line managers and actioned by the Internal IT. (Access Control Process 9)	Confirmed that access to data stored on the network is restricted using appropriate permissions. Users are assigned with Functional Group/s with appropriate levels of access permission aligned with their duties. Observed access settings and confirmed that only IT technicians can amend an individual’s access permissions outside of the SharePoint Team access. Observed authentication setup and confirmed that multi-factor authentication is used to access data remotely. Inspected a sample of accesses, reviewed and confirmed that staff profiles are reviewed on a quarterly basis by the staff member’s manager and are amended by IT when a staff member changes roles or leaves the company. We were not able to inspect any evidence of a user with a role change for the period under review. For the sampled new users, confirmed that user access required line manager authorisation prior to user access being actioned by IT. **No exceptions noted.**

Control Objectives	Audit Finding
8. Maintaining integrity of the systems	
Access to the administration system is controlled windows authentication, two factor authentication and utilising Privileged Identity Management; where possible this requires users to enable Administrative Roles when required. Segregation of duties and rules are enforced by security profiles built into the administration system. Profiles are assigned to authorised individuals and aligned to their roles and responsibilities. Associated with each administrator is a security profile which determines schemes to which they have access, functionality they can access, member records they can access, whether they are permitted to amend data or view data only.	Observed access settings and confirmed that Microsoft Azure AD Authentication is in place and multi-factor authentication is enforced on all users. Microsoft Azure's Privileged Identity Management is utilised to control access to the administration system. Confirmed that only IT administrators can change access permissions. Observed user access setup and confirmed that users are assigned access through functional groups. These groups are maintained with appropriate levels of access permissions, ensuring segregation of duties and rules are enforced. Each group is set up that gives user access only to the access required in line with their roles and responsibilities. Verified through observation that different levels of security profiles are built into the administration system restricting unauthorised access. **No exceptions noted.**
The audit trail facility records changes made to the data, including who made the changes and when, providing integrity and resilience to the information processing environment, commensurate with the value of the information held, information processing performed and external threats.	For the sampled users, inspected the audit trail facilities in place and confirmed that an audit trail of changes made to data, including who made the changes and when, is kept. **No exceptions noted.**
All IT processing is carried out in real time. Spence utilises SharePoint and Azure AD guest accounts for controlling access to SharePoint Online. Conditional access controls are in place for all guests account to force the use of Multi Factor Authentication.	Observed a visual timeline of online processing activity by users and confirmed that all processing is carried out in real-time. Observed the SharePoint secure portal and confirmed that it is used for the sharing of information externally where user access rights are confirmed. Through observation of a sample of SharePoint and AD guest accounts, confirmed that Spence utilises these to control access to SharePoint Online. Inspected the Azure AD Authentication methods and confirmed that multi-factor authentication is used to access data remotely. **No exceptions noted.**

Control Objectives	Audit Finding
All external access to the network is authorised internally by IT and persons holding an elevated role. Remote access to internal systems is granted by IT Department and connections can only be made through Windows Virtual Desktop. The company contracts WaveNet to host a Firewall within its datacentre to control port access in and out of the business. All email traffic is routed, scanned and archived by a third party, Mimecast, which filters out any email threats i.e., viruses/spyware and inappropriate content. External email tagging is also implemented. Inappropriate content also triggers a rules-based alerting system that keeps staff members aware of any trends requiring action. Windows Defender software is installed on all servers, desktops and laptops and is designed to keep users safe from viruses and other forms of on-line malicious threats. Anti-Virus software is installed on all servers, desktops and laptops and is designed to keep users safe from viruses and other forms of on-line malicious threats.	For the sampled external access, confirmed that network access is required to be authorised by the Head of IT. Confirmed that remote access connections can only be made through Windows Virtual Desktop (WVD). Inspected the Windows Defender software and confirmed that it is used to provide anti-virus protection and that it is installed on all devices, and for the sampled devices, had no active malware. Observed Microsoft Outlook email settings and confirmed that Mimecast is used to monitor email traffic and remove threats. Inspected the WaveNet agreement in place and confirmed that WaveNet is used to provide firewall protection. Inspected the Windows Defender software and the Anti-Virus software and confirmed that it is used to provide anti-virus protection and that it is installed on all devices, and for the sampled devices had no active malware. Inspected the Default Windows Defender Anti-Virus Policy and confirmed that scanning of all incoming and outgoing traffic, including emails. Confirmed through observation that Mimecast is used to monitor email traffic and removes any threats based on a rules-based alerting system which provides inappropriate content alerts. **No exceptions noted.**
9. Maintaining and developing systems hardware and software	
Our pension administration technologies have not required migration or modification of data in recent years. Any such process would follow our change management procedures as described in Maintaining and developing systems hardware and software. For new scheme implementations please refer to Accepting clients. For periodic and ad-hoc data loads please refer to Maintaining financial and other records.	For the sampled changes for pension administration technologies (i.e., Mantle), it was confirmed that change management procedures described in Maintaining and developing systems hardware and software were followed. Appropriate development, testing and approval were performed accordingly, and relevant documents or records were maintained. Confirmed for the sampled changes for new scheme implementation, acceptance from clients is required. Confirmed for the sampled changes for data loads, financial and other records are maintained. **No exceptions noted.**

Control Objectives	Audit Finding
Any changes to existing, or the implementation of new, infrastructure and systems follows the Operational Change Control process outlined in Operations Security Process (Process 12). A major change will typically be a planned implementation, and this will typically be discussed at IT subcommittee. When a major change is required business impact is reviewed and formal sign-off and authorisation is required. (Operations Security Process 12)	Confirmed that Operations Security Policy outlined Change Management Procedures which provide guidelines on any changes to existing or the implementation of new infrastructure and systems. For the sampled changes, it was confirmed that change management procedures described in the policy were followed. Appropriate development, testing and approval were performed accordingly, and relevant documents or records were maintained. Observed that an internal change log is maintained within the IT Service Desk and discussed at the IT subcommittee as per the change management procedures. Confirmed that sampled major changes includes business impact review, formal sign-off and authorisation before implementation to production. **No exceptions noted.**
Spence has also adopted an effective System Acquisition, Development, and Maintenance process (Process 14). Controls are in place to ensure the installation and upgrading of operational software on each operating system. In addition, user profiles are employed to ensure that only IT colleagues are authorised to perform installations or upgrades. This requires elevated permissions.	Inspected the System Acquisition, Development, and Maintenance Process and confirmed that Spence has an effective process in place. For the sampled changes, confirmed that processes defined are followed accordingly. For the sampled devices, confirmed that they are configured with the latest software update. Confirmed that automatic control in place for application updates for iOS, MacOS and Windows. Inspected the configuration of the Azure Patch Management, which is managed through InTune and Microsoft Azure, and confirmed that iOS, MacOS and Windows updates are rolled out on a regular basis to all computers on the network. Inspected the patch management settings and confirmed that WVD is patched monthly except for security and critical patches which are deployed within 14 working days of release. Only authorised IT colleagues with administrative roles are permitted to perform installations or upgrades. **No exceptions noted.**
Any maintenance is performed by authorised representatives from the corresponding software/ support company and is pre-arranged. Notice is given to colleagues of any downtime to the network that is required for the maintenance of software. Any software upgrades are performed only if there is a requirement to do so, or suitably long enough after the release, to ensure any bugs or vulnerabilities have been ironed out. If new software potentially introduces any element of risk, then the risk will be assessed and its advantages of functionality will be subject to continued monitoring and/or isolated.	Inspected the HTG agreement in place and confirmed that Citrix application updates are provided by managed service provider HTG. Updates are not authorised to be completed between the hours of 8:00-18:00. Confirmed through observation of user profiles that Internal IT members are the only authorised individuals that can perform installations or upgrades. Confirmed that maintenance is performed by authorised representatives from HTG and is pre-arranged. Verified for a sample of notifications sent to staff informing them of system maintenance.

Control Objectives	Audit Finding
For Anti-virus protection, Spence has implemented Windows Defender Advanced Threat Protection (ATP). This ensures appropriate controls and procedures are in place to protect the integrity of system software and information from compromise following the introduction of malicious software. It shall be considered a serious disciplinary offence for any member of the Group, either permanent or temporary, to take any action which places the Group in danger of infection by malicious software, viruses or any other such threat. Mimecast/Exchange Online Advanced Threat Protection (ATP) is in place to scan e-mail attachments for malware. A patch management cycle is in place to reduce the vulnerabilities that could be exploited by malware. A business continuity plan is in place to help the organisation recover from malware attacks. Appropriate levels of control are implemented to minimise the likelihood of a virus infection, and to minimise the impact should an infection occur. Controls are deployed as follows: — All virus controls shall be updated as per manufacturer's instructions and kept current. — The use of unauthorised software on company property is prohibited. — Workstations and systems shall be checked daily/on demand by Microsoft Defender. — Contingency plans shall be developed to ensure an effective organisational reaction to a virus incident. — Training to ensure that all users are aware of their responsibilities and to fulfil them. — A Security and Confidentiality Policy has been distributed along with the Employee Handbook to ensure staff awareness of roles and responsibilities to information security.	Inspected the Information System Acquisition, Development, and Maintenance Process and confirmed software upgrades are performed only if there is a requirement to do so, or suitably long enough after the release, to ensure any bugs or vulnerabilities have been ironed out. Further confirmed that new software will be assessed for any elements of risk and any advantages of functionality will be subject to continued monitoring and / or isolated. Confirmed through review of the disciplinary procedure and the information security policy, that it is considered a serious disciplinary offence for any member of the Group, permanent or temporary, to take any action which places the Group in danger of infection by malicious software, viruses, or any other threat. Inspected the Windows Defender software and confirmed that it is used to provide anti-virus protection and that it is installed on all devices, and at the time of the walkthrough all devices had no active malware. Observed Microsoft Outlook email settings and confirmed that Mimecast is used to monitor email traffic and remove threats. Inspected the configuration of the Azure Patch Management, which is managed through InTune and Microsoft Azure, and confirmed that iOS, MacOS and Windows updates are rolled out on a regular basis to all computers on the network. Inspected the patch management settings and confirmed that WVD is patched monthly except for security and critical patches which are deployed within 14 working days of release. Inspected the Business Continuity Plan and confirmed that it details processes to enable recovery from loss of information assets (which may be the result of, for example, natural disasters, accidents, equipment failures, and deliberate actions) and to minimise the impact of incidents to an acceptable level through a combination of preventive and recovery controls. Verified for a sample of new joiners that mandatory training was completed, and Information Security and refresher training is provided every two years. Verified for the same sample of new joiners in 2022 that the Security and Confidentiality policy had been signed to confirm their understanding of the policy and their responsibilities regarding information security. **No exceptions noted.**

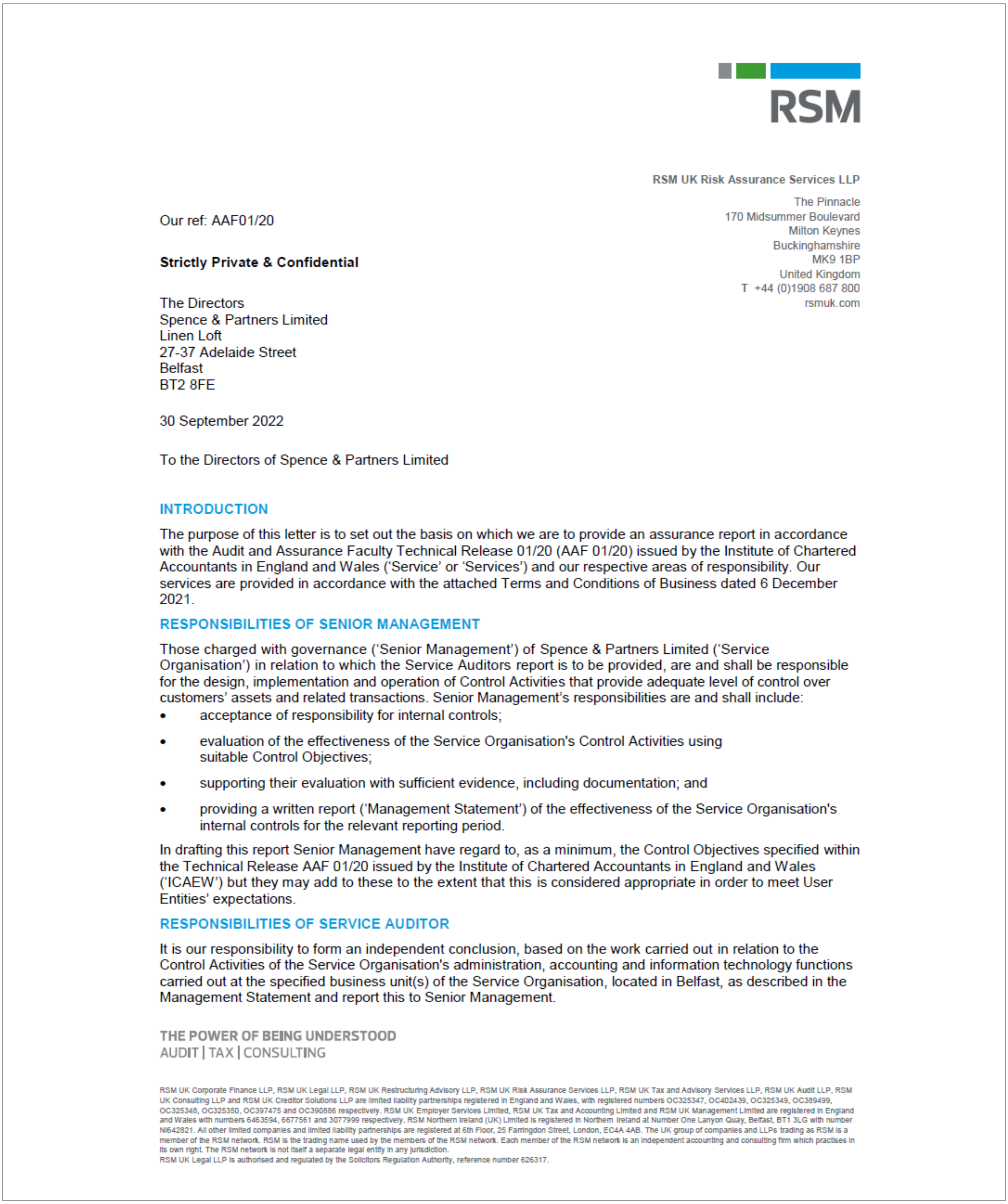
Control Objectives	Audit Finding
Windows updates are rolled out periodically to all computers on the network. Development of systems is facilitated by an appropriate rollback strategy.	Inspected the configuration of the Azure Patch Management, which is managed through InTune and Microsoft Azure, and confirmed that windows updates are rolled out on a regular basis to all computers on the network. For the sampled changes, confirmed that development is performed if needed and appropriate rollback strategy is defined within the ticket. **No exceptions noted.**
10. Recovery from processing interruptions	
Spence works securely within a virtual environment. In the event of the failure of a server, functionality is transferred to other servers. The IT infrastructure facilitates the continuation of business operations from any location in the event of multiple disaster scenarios. **Backup and Restore Technology** All servers in Azure are backed up on a daily basis at 22:00 UTC. SQL Databases are backed up in Full starting at 19:30 UTC with transaction log backups running continuously every hour on supported databases. Recovery snapshots are held for two days, and daily backups are retained for 30 days, with Spence retaining a weekly backup for three months. Spence utilises Azure Site Recovery to replicate data between Azure datacentres (DC). The primary Azure DC is UK South, and DR DC is UK West Recovery Point Objective ("RPO") is under one hour with a Recovery Time Objectives ("RTO") of under four hours for the entire virtual estate.	Inspected the backup schedule for servers on Azure and confirmed a daily back up process is in place and scheduled to run at 22:00 UTC. Inspected the backup schedule for SQL databases and confirmed that they are backed up in Full starting at 19:30 UTC with transaction log backups running continuously every hour on supported databases. Further, confirmed that it is set to retain instant restore recovery snapshots for up to 2 days, up to 30 days of the daily backups, and up to 3 months for the weekly backups. Observed the Microsoft Azure Recovery Services and confirmed that two geographically separate data centres are used to host the services to provide additional resilience. A replica of the primary data centre (UK South) is in place and is used in the event of disaster recovery (UK West). Observed within Microsoft Azure Recovery Services that the replication was noted to be healthy and protected with the last failover test performed on 21st November 2022 and no configuration issues. Inspected the Business Continuity Plan and confirmed the Recovery Point Objective ("RPO") is one hour and Recovery Time Objective is under four hours for the entire virtual estate. **No exceptions noted.**
The Business Continuity Plan ("BCP") sets out the processes and procedures used to counteract interruptions to business activities and to protect critical business processes from the effects of failures or disasters affecting our information and broader IT systems, and to ensure their timely resumption.	Inspected the Business Continuity Plan and confirmed that it details processes to enable recovery from loss of information assets (which may be the result of, for example, natural disasters, accidents, equipment failures, and deliberate actions) and to minimise the impact of incidents to an acceptable level through a combination of preventive and recovery controls**.**

Control Objectives	Audit Finding
Replication and Recovery Technology Spence has invested in Azure Site Recovery which enables automated data recovery, failover, and failback of full or partial infrastructures dependent on the failure type and recovery need. The BCP details processes to enable recovery from loss of information assets (which may be the result of, for example, natural disasters, accidents, equipment failures, and deliberate actions) and to minimise the impact of incidents to an acceptable level through a combination of preventive and recovery controls. The critical business processes and information security management requirements of business (operations, Spence third party resourcing, information / data hard copy and facilities) have also been included.	Inspected the BCP Testing Schedule and results and confirmed failover tests of Azure (UK South) to Azure (UK West) have been conducted in 2022 with recovery times achieving a Recovery Point Objective ("RPO") of 1 hour. Further, confirmed that disaster recovery testing of the IT infrastructure is completed on a 90-day cycle and is in line with BCP plan. **No exceptions noted.**
The BCP provides a framework for responses to specific areas of vulnerability and threat in the event of incidents of catastrophic failure as well as other unforeseen events. Our BCP Team is ultimately responsible for designing and maintaining the BCP, which is managed and implemented by the BCP Manager and a deputy. A command structure is in place to manage an incident. We have adopted the Gold/Silver command structure, as widely used elsewhere in contingency planning. This ensures an effective division of duty between command and control and operational recovery responsibilities. Key Spence third party resources are included in this command structure (Business Continuity Management Process 17); Business Continuity Plan, BCP Testing Schedule and results 2011 to 2022).	Inspected a copy of the Group Business Continuity Plan and confirmed that it is in place and contains comprehensive information in relation to BCP roles and responsibilities, scenarios, response strategies, plan activation criteria, critical business process, information security requirements and disaster recovery requirements. Further, confirmed that command structure is in place with roles and responsibilities for gold and silver team members (which include third-party resources) clearly outlined and allocated. **No exceptions noted.**
Hard copies of the BCP and supporting documents are held securely and confidentially off site by the BCP Manager and Gold team members. The BCP and supporting documents for the Information Security Management System are in line with ISO 27001 framework and guidelines taken from the BS25999 part 2 Business Continuity Management Standard. All plans are based around a recovery point, time and capacity objectives that have been agreed with the business. Maintenance of the plans is controlled as part of the evaluation of each disaster recovery event. (Organisation of Information Security Process 6).	Confirmed that copies of the Business Continuity Plan are held securely and confidentially offsite by the BCP Manager and Gold Team members, including the deputies of these team members. Inspected the Business Continuity Plan and confirmed that the BCP documents are in line with ISO 27001 framework and guidelines taken from the BS25999 part 2 Business Continuity Management Standard. Confirmed that the plan is based around a recovery point, time, and capacity objectives that have been agreed with the business. Inspected the Organisation of Information Security Process and confirmed that the maintenance of the plans is controlled as part of the evaluation of each disaster recovery event. **No exceptions noted.**

Control Objectives	Audit Finding
Spence works securely within a virtual environment. In the event of the failure of a server, functionality is temporarily transferred to other servers via automated dynamic resource allocation processes minimising interruption to business operations. The IT infrastructure facilitates the continuation of business operations from any location in the event of multiple disaster scenarios.	Observed the Microsoft Azure Recovery Services and confirmed that two geographically separate data centres are used to host the services to provide additional resilience. A replica of the primary data centre (UK South) is in place and is used in the event of disaster recovery (UK West). Inspected the BCP Testing Schedule and results and confirmed that a failover test was completed during the audit period. **No exceptions noted.**
11. Managing and Monitoring Compliance and Outsourcing	
Spence utilises Log Analytics to monitor service health. Azure Spence outsources WVD managing and monitoring to CloudDirect. Documented service level agreements are in place, covered by appropriate contracts and monitored by the Directors. Regular governance and service review meetings are held along with third party audits conducted on a regular basis. Spence also employ third-party penetration and security experts Check accredited providers to audit the network infrastructure annually. (Process 6 Organisation of Information Security and Process 10 Cryptography).	Observed dashboards Azure Monitor, Azure Sentinel and Cloud App Security and confirmed that these tools are used to monitor service health. Confirmed that a service level agreement is in place between Spence and HTG and monitored by the Directors. For the sampled monthly service review packs, confirmed that regular governance and service review meetings are held with third parties with any major issues escalated to the Board meetings. Inspected the IT Health Check & Vulnerability Assessment (penetration testing), and a Cyber Essentials Plus audits and confirmed that these audits were completed during 2022. Further, confirmed through inspection of these audit reports that an accredited provider was used to perform these audits. **No exceptions noted.**

Appendices

Letter of Engagement



RSM

RSM UK Risk Assurance Services LLP

The Pinnacle
170 Midsummer Boulevard
Milton Keynes
Buckinghamshire
MK9 1BP
United Kingdom
T +44 (0)1908 687 800
rsmuk.com

Our ref: AAF01/20

Strictly Private & Confidential

The Directors
Spence & Partners Limited
Linen Loft
27-37 Adelaide Street
Belfast
BT2 8FE

30 September 2022

To the Directors of Spence & Partners Limited

INTRODUCTION

The purpose of this letter is to set out the basis on which we are to provide an assurance report in accordance with the Audit and Assurance Faculty Technical Release 01/20 (AAF 01/20) issued by the Institute of Chartered Accountants in England and Wales (‘Service’ or ‘Services’) and our respective areas of responsibility. Our services are provided in accordance with the attached Terms and Conditions of Business dated 6 December 2021.

RESPONSIBILITIES OF SENIOR MANAGEMENT

Those charged with governance (‘Senior Management’) of Spence & Partners Limited (‘Service Organisation’) in relation to which the Service Auditors report is to be provided, are and shall be responsible for the design, implementation and operation of Control Activities that provide adequate level of control over customers’ assets and related transactions. Senior Management’s responsibilities are and shall include:

- acceptance of responsibility for internal controls;
- evaluation of the effectiveness of the Service Organisation's Control Activities using suitable Control Objectives;
- supporting their evaluation with sufficient evidence, including documentation; and
- providing a written report (‘Management Statement’) of the effectiveness of the Service Organisation's internal controls for the relevant reporting period.

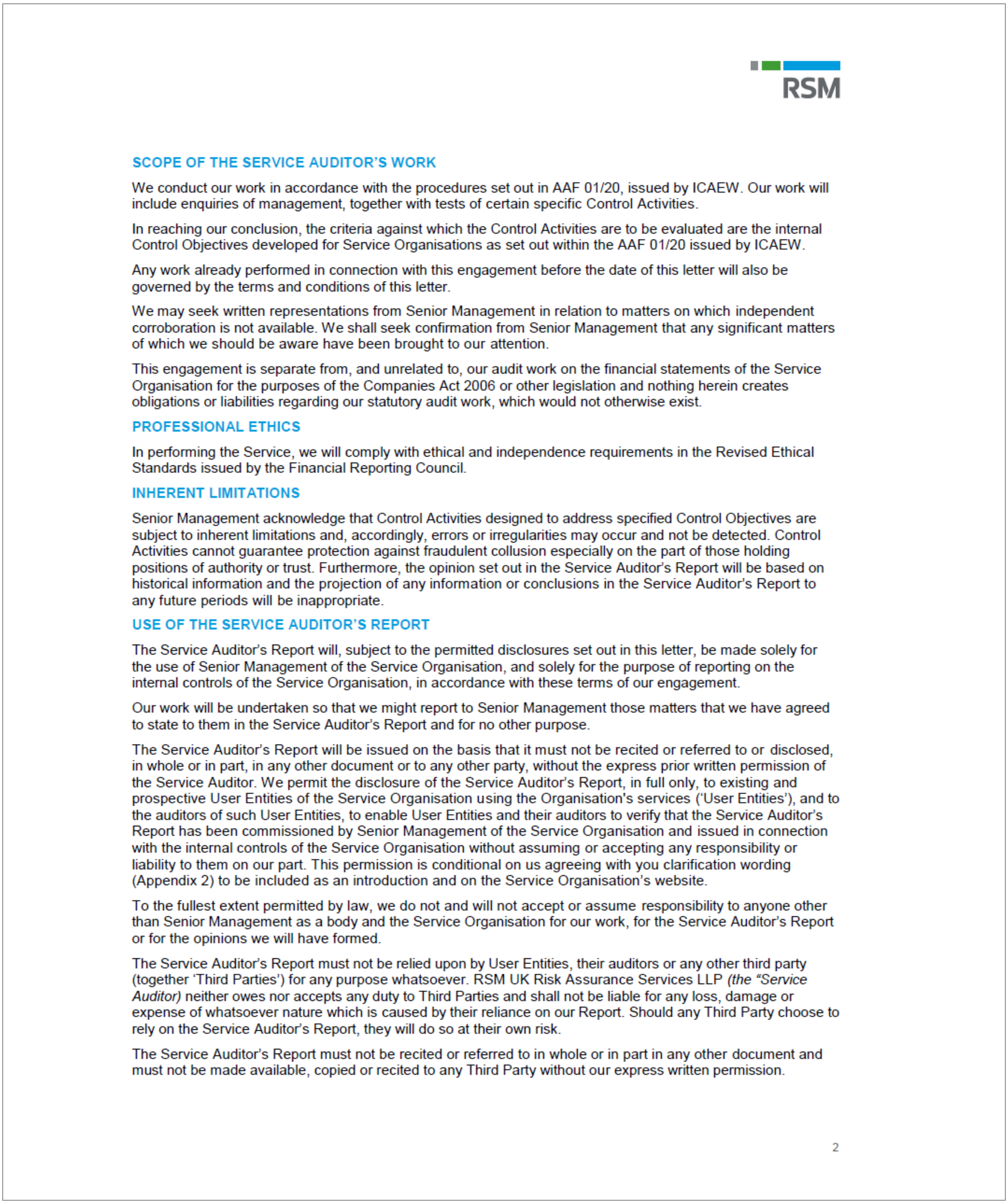
In drafting this report Senior Management have regard to, as a minimum, the Control Objectives specified within the Technical Release AAF 01/20 issued by the Institute of Chartered Accountants in England and Wales (‘ICAEW’) but they may add to these to the extent that this is considered appropriate in order to meet User Entities’ expectations.

RESPONSIBILITIES OF SERVICE AUDITOR

It is our responsibility to form an independent conclusion, based on the work carried out in relation to the Control Activities of the Service Organisation's administration, accounting and information technology functions carried out at the specified business unit(s) of the Service Organisation, located in Belfast, as described in the Management Statement and report this to Senior Management.

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

RSM UK Corporate Finance LLP, RSM UK Legal LLP, RSM UK Restructuring Advisory LLP, RSM UK Risk Assurance Services LLP, RSM UK Tax and Advisory Services LLP, RSM UK Audit LLP, RSM UK Consulting LLP and RSM UK Creditor Solutions LLP are limited liability partnerships registered in England and Wales, with registered numbers OC325347, OC402439, OC325349, OC389499, OC325348, OC325350, OC397475 and OC390886 respectively. RSM UK Employer Services Limited, RSM UK Tax and Accounting Limited and RSM UK Management Limited are registered in England and Wales with numbers 6463594, 6677561 and 3077999 respectively. RSM Northern Ireland (UK) Limited is registered in Northern Ireland at Number One Lanyon Quay, Belfast, BT1 3LG with number NI642821. All other limited companies and limited liability partnerships are registered at 6th Floor, 25 Farringdon Street, London, EC4A 4AB. The UK group of companies and LLPs trading as RSM is a member of the RSM network. RSM is the trading name used by the members of the RSM network. Each member of the RSM network is an independent accounting and consulting firm which practises in its own right. The RSM network is not itself a separate legal entity in any jurisdiction.
RSM UK Legal LLP is authorised and regulated by the Solicitors Regulation Authority, reference number 626317.



SCOPE OF THE SERVICE AUDITOR'S WORK

We conduct our work in accordance with the procedures set out in AAF 01/20, issued by ICAEW. Our work will include enquiries of management, together with tests of certain specific Control Activities.

In reaching our conclusion, the criteria against which the Control Activities are to be evaluated are the internal Control Objectives developed for Service Organisations as set out within the AAF 01/20 issued by ICAEW.

Any work already performed in connection with this engagement before the date of this letter will also be governed by the terms and conditions of this letter.

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

This engagement is separate from, and unrelated to, our audit work on the financial statements of the Service Organisation for the purposes of the Companies Act 2006 or other legislation and nothing herein creates obligations or liabilities regarding our statutory audit work, which would not otherwise exist.

PROFESSIONAL ETHICS

In performing the Service, we will comply with ethical and independence requirements in the Revised Ethical Standards issued by the Financial Reporting Council.

INHERENT LIMITATIONS

Senior Management acknowledge that Control Activities designed to address specified Control Objectives are subject to inherent limitations and, accordingly, errors or irregularities may occur and not be detected. Control Activities cannot guarantee protection against fraudulent collusion especially on the part of those holding positions of authority or trust. Furthermore, the opinion set out in the Service Auditor's Report will be based on historical information and the projection of any information or conclusions in the Service Auditor's Report to any future periods will be inappropriate.

USE OF THE SERVICE AUDITOR'S REPORT

The Service Auditor's Report will, subject to the permitted disclosures set out in this letter, be made solely for the use of Senior Management of the Service Organisation, and solely for the purpose of reporting on the internal controls of the Service Organisation, in accordance with these terms of our engagement.

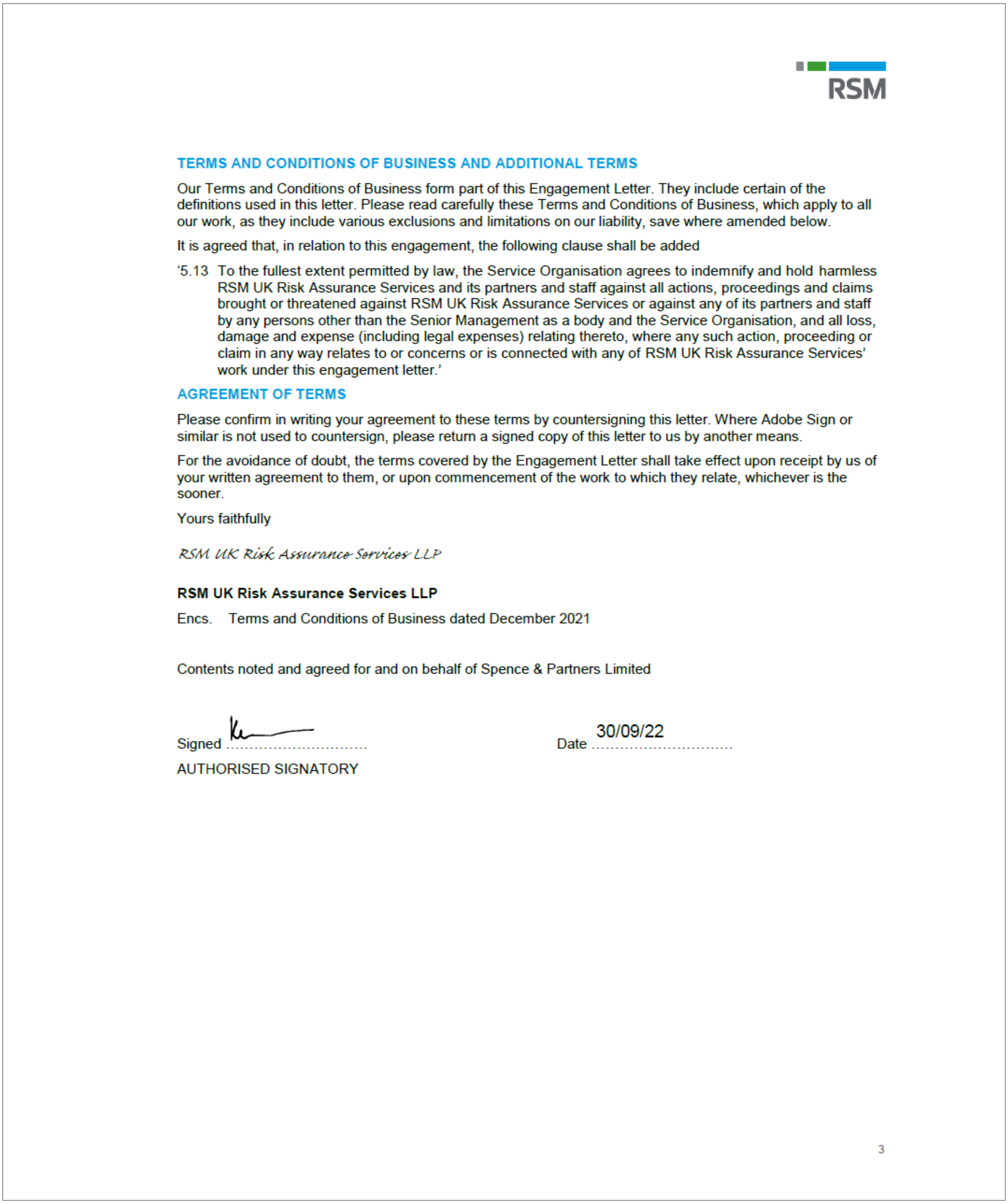
Our work will be undertaken so that we might report to Senior Management those matters that we have agreed to state to them in the Service Auditor's Report and for no other purpose.

The Service Auditor's Report will be issued on the basis that it must not be recited or referred to or disclosed, in whole or in part, in any other document or to any other party, without the express prior written permission of the Service Auditor. We permit the disclosure of the Service Auditor's Report, in full only, to existing and prospective User Entities of the Service Organisation using the Organisation's services ('User Entities'), and to the auditors of such User Entities, to enable User Entities and their auditors to verify that the Service Auditor's Report has been commissioned by Senior Management of the Service Organisation and issued in connection with the internal controls of the Service Organisation without assuming or accepting any responsibility or liability to them on our part. This permission is conditional on us agreeing with you clarification wording (Appendix 2) to be included as an introduction and on the Service Organisation's website.

To the fullest extent permitted by law, we do not and will not accept or assume responsibility to anyone other than Senior Management as a body and the Service Organisation for our work, for the Service Auditor's Report or for the opinions we will have formed.

The Service Auditor's Report must not be relied upon by User Entities, their auditors or any other third party (together 'Third Parties') for any purpose whatsoever. RSM UK Risk Assurance Services LLP *(the "Service Auditor)* neither owes nor accepts any duty to Third Parties and shall not be liable for any loss, damage or expense of whatsoever nature which is caused by their reliance on our Report. Should any Third Party choose to rely on the Service Auditor's Report, they will do so at their own risk.

The Service Auditor's Report must not be recited or referred to in whole or in part in any other document and must not be made available, copied or recited to any Third Party without our express written permission.



TERMS AND CONDITIONS OF BUSINESS AND ADDITIONAL TERMS

Our Terms and Conditions of Business form part of this Engagement Letter. They include certain of the definitions used in this letter. Please read carefully these Terms and Conditions of Business, which apply to all our work, as they include various exclusions and limitations on our liability, save where amended below.

It is agreed that, in relation to this engagement, the following clause shall be added

'5.13 To the fullest extent permitted by law, the Service Organisation agrees to indemnify and hold harmless RSM UK Risk Assurance Services and its partners and staff against all actions, proceedings and claims brought or threatened against RSM UK Risk Assurance Services or against any of its partners and staff by any persons other than the Senior Management as a body and the Service Organisation, and all loss, damage and expense (including legal expenses) relating thereto, where any such action, proceeding or claim in any way relates to or concerns or is connected with any of RSM UK Risk Assurance Services' work under this engagement letter.'

AGREEMENT OF TERMS

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

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

Yours faithfully

RSM UK Risk Assurance Services LLP

RSM UK Risk Assurance Services LLP

Encs. Terms and Conditions of Business dated December 2021

Contents noted and agreed for and on behalf of Spence & Partners Limited

Signed .... Date 30/09/22 ....

AUTHORISED SIGNATORY

SPENCE

Belfast

Linen Loft
27-37 Adelaide Street
Belfast BT2 8FE

T: +44 (0)28 9041 2000

Bristol

Castlemead
Lower Castle Street
Bristol BS1 3AG

T: +44 (0)117 959 5002

Glasgow

The Culzean Building
36 Renfield Street
Glasgow G2 1LU

T: +44 (0)141 331 1004

London

46 New Broad Street
London
EC2M 1JH

T: +44 (0)20 7495 5505

Manchester

St James Tower
7 Charlotte Street
Manchester M1 4DZ

T: +44 (0)161 641 6312

Birmingham

Edmund House
12-22 Newhall Street
Birmingham B3 3AS

T: +44 (0)121 389 2314

Leeds

Princes Exchange
Princes Square, Leeds
West Yorkshire LS1 4HY

T: +44 (0)113 426 4487

spenceandpartners.co.uk

Authorised and regulated by the Financial Conduct Authority. No. NI37760