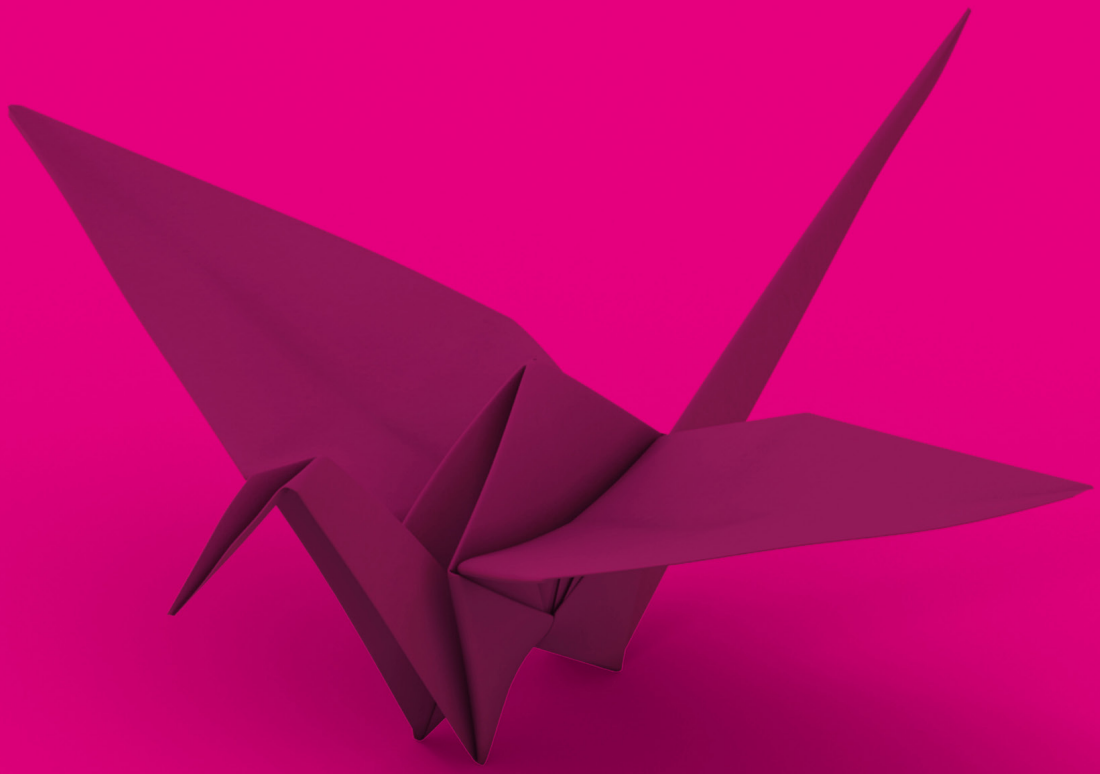
Assurance Report on Internal Controls

(AAF 01/06 and ISAE 3402)

For the period 1 January to
31 December 2020



Dalriada.
A better way

Statement of Reporting Accountants

Number One Lanyon Quay
Belfast
BT1 3LG

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

rsmuk.com

Statement of Reporting Accountants

Our Report, as set out at page 26, has been prepared solely in accordance with terms of engagement agreed by the Directors of Dalriada Trustees Limited ("the Directors") with RSM Northern Ireland (UK) Limited and for the confidential use of Dalriada Trustees Limited ("the Organisation") and solely for the purpose of reporting on the internal controls and providing an independent conclusion on the Directors' report set out at page 24 hereof. Our Report must not be relied upon by the Organisation for any other purpose whatsoever.

We have, exceptionally, agreed to permit the disclosure of our Report on the Organisation's website, in full only, to customers and potential customers of the Organisation using the Organisation's services ("Customers") and to the auditors of such Customers, to enable Customers and their auditors to verify that a report by reporting accountants has been commissioned by the Directors of the Organisation and issued in connection with the internal controls of the Organisation without assuming or accepting any responsibility or liability to them on our part.

Our Report must not be relied upon by Customers, their auditors or any other third party (together "Third Parties") for any purpose whatsoever. RSM Northern Ireland (UK) Limited 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 our Report, they will do so at their own risk.

Our 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.

RSM Northern Ireland (UK) Limited

RSM Northern Ireland (UK) Limited

Contents

1 | Introduction

1 Introduction

The Directors of Dalriada Trustees Limited ("Dalriada") are pleased to present our report detailing the control procedures that are in place for our Trustee and Master Trust services.

This report covers the year ended 31 December 2020 and has been prepared in accordance with the Technical Release AAF 01/06 "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").

As the control objectives are consistent with The International Standard on Assurance Engagements ("ISAE") 3402, Dalriada is reporting on both standards for this reporting period.

The 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.

The control objectives are set out on pages 30 to 33 and we demonstrate how we meet these on pages 35 to 62 These measures have been audited and reported upon by RSM Northern Ireland (UK) Limited. This is the seventh such report we have published.

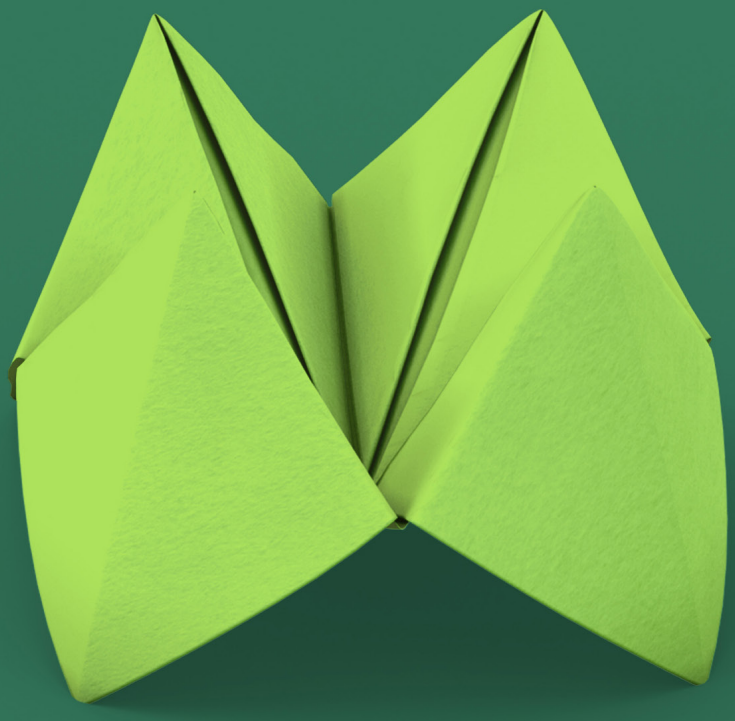
Dalriada is a privately owned UK company that acts as a professional trustee. Our organisation is managed by seven Directors who supervise the activities of a number of highly experienced and qualified pensions administrators and support staff. We have clients throughout the UK serviced from our offices in Belfast, Birmingham, Bristol, Glasgow, Leeds, London, and Manchester.

Dalriada provides a range of pension scheme trustee services which include the provision of administration, pension fund accounting, pension data audit, and pension benefit audit services to a range of pension scheme clients. In addition, we have specialist expertise in remedial pension scheme data audit work, which 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.

Dalriada was appointed to the PPF's Trustee Advisory Panel ("TAP") in September 2013. Our specialist PPF and FAS team handles all aspects of the assessment process including project management, administration and pension fund accounting.

Dalriada won the 'Independent Trustee Firm of the Year' category in the UK Pensions Age Awards 2020 and the Corporate Adviser Awards 2020 for 'Best Independent DC Trustee'.

2 | Background and Organisation Structure



2 Background and Organisation Structure

Dalriada Trustees is a professional pension scheme trustee company.

Our individual owners have been intimately involved every step of the way since Dalriada was founded in 2003 and continue to work full-time as professional trustees within the Dalriada team. Our owners' overriding business objective is to provide interesting and truly worthwhile careers for our people and this ethos has facilitated the recruitment and retention of one of the strongest professional trustee teams in the industry.

Our team includes younger members who have been acting as trustees from the very outset of their careers to veterans with over 50 years' experience in the pensions industry, but they are all career trustees working on a full-time or nearly full-time basis.

Many decisions taken by trustee boards are finely balanced. At Dalriada we firmly believe that trustee boards make better, more robust decisions where they reflect the diversity of scheme members and of society more generally. The Dalriada team is diverse in terms of gender, age and ethnicity as well as professional background.

We apply our considerable specialist skills to work with pension scheme sponsors to deliver the best possible outcomes for pension scheme members. Dalriada has been entrusted with the stewardship of many billions of pounds invested on behalf of thousands of pension scheme members and we take this responsibility very seriously. We cannot eliminate investment risk, but we have the expertise to manage it. Our approach to investment places sustainability at the forefront of our thinking, and we always seek to ensure Environmental, Social and Governance ("ESG") factors are applied in a practical way that takes on board many of the concerns of our members.

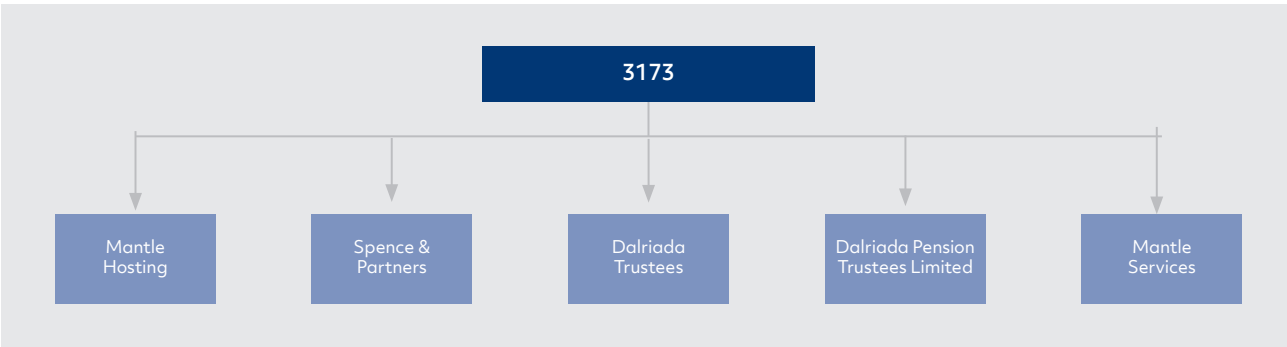
Dalriada applies process and technology to deliver more efficient and better service to our members. We work closely with partners committed to the use of Financial Technology ("Fintech") to develop online access for members, where possible and this is their preference, timely reporting and best in class risk management.

Since our inception we have provided trustee services to pension schemes at varying stages of their development including on-going schemes, schemes in the process of winding up and schemes in PPF and FAS Assessment.

Dalriada has a number of sister companies. Spence & Partners is a professional firm of actuaries, pension consultants, pension scheme information technology ("IT") specialists and administrators. Dalriada Pension Trustees Limited operates as a separate professional trustee company to provide professional trusteeship services to pension schemes in Ireland. Mantle Hosting Limited (formerly The Pensions Hosting Limited) is an IT software business providing web-based pension administration and actuarial services. Mantle Services Limited (formerly Veratta Limited) is a privately owned UK firm of data management, software development, information security and IT specialists with a focus on the pensions and financial services industry.

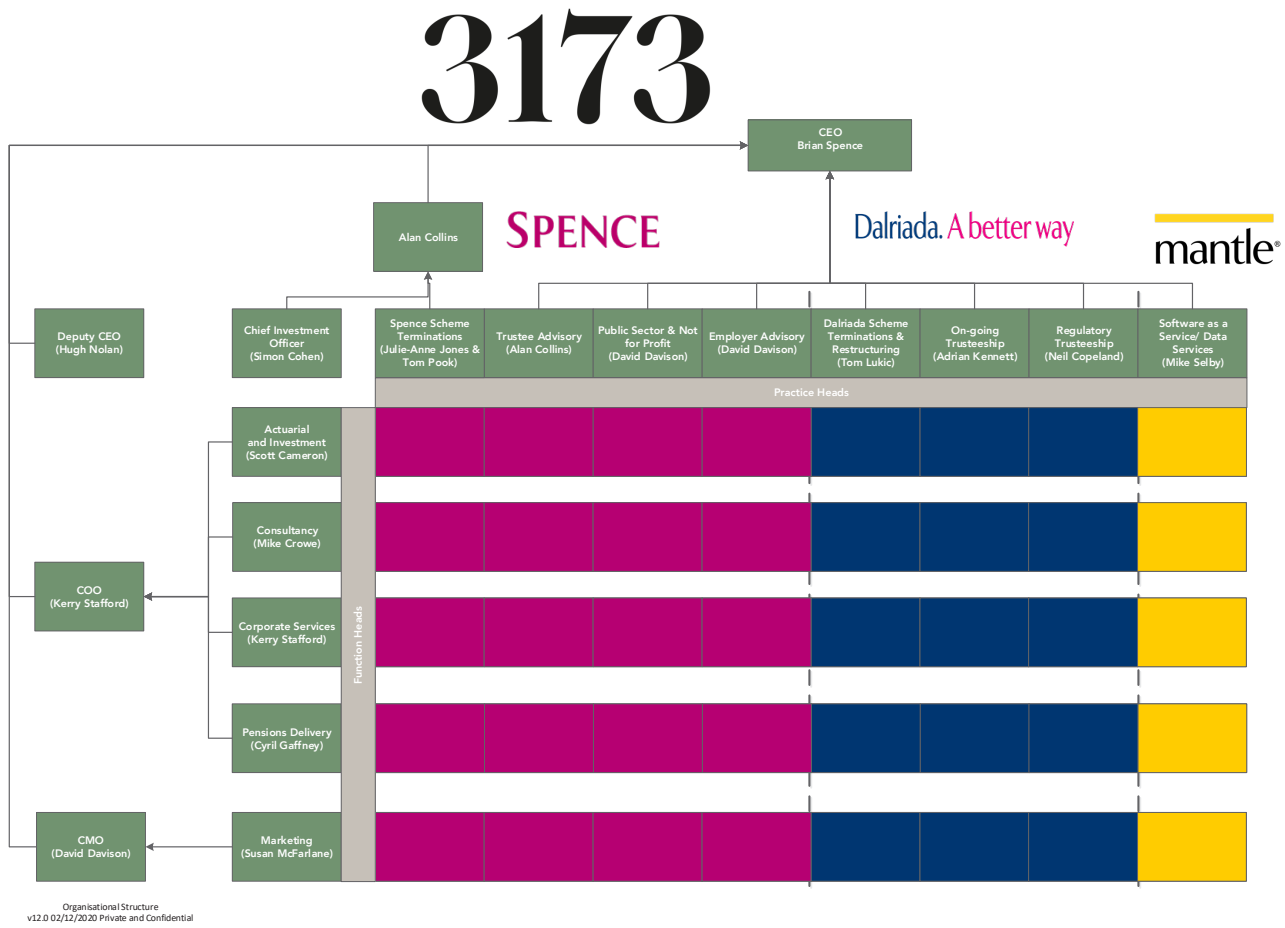
Our clients are based throughout the UK and Ireland and are serviced from our offices in Belfast, Birmingham, Bristol, Glasgow, Leeds, London, and Manchester.

3173 Limited (formerly Ellcon Investments Limited), is the holding company for the Group.



Under our group's matrix management structure, Dalriada is able to draw on the experience of over 149 pension professionals across a range of disciplines. Specialist members of staff include, accountants, actuaries, administrators, consultants, covenant advisors, investment, legal, pension fund pension database experts 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 structure is illustrated in the table below as a two dimensional matrix.



Our Practice Heads across all companies are responsible for all aspects of the development of services to a particular market segment.

Practice Heads take overall responsibility for the delivery of 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 business 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 trustee representative is key to our working relationship with clients, and they have overall responsibility for the service provided to their clients. The trustee representatives 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., Risk and Audit, HR and Business Support resources.

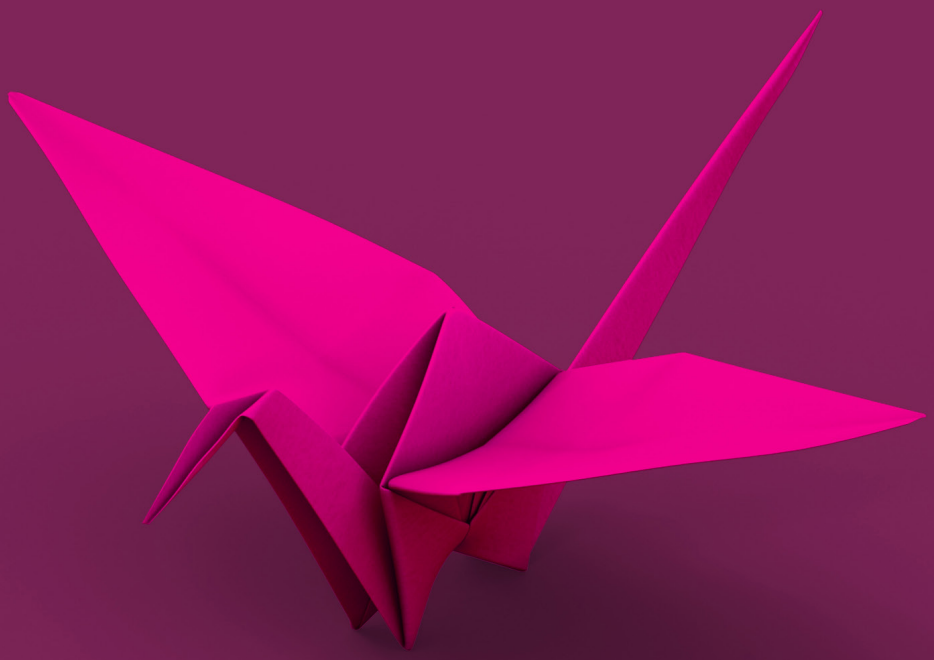
The Consultancy, Pensions Delivery and Actuarial & Investment Function Heads report to Kerry Stafford, Chief Operating Officer. The Marketing Function Head reports to David Davison, our Chief Marketing Officer. The Practice Heads for Spence Scheme Terminations and the Chief Investment Officer report to Alan Collins, a Director of Spence. Hugh Nolan, our Deputy CEO and the remaining Practice Heads across all Companies report to our Chief Executive Officer, 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 Dalriada Board is supported by a number of advisory groups:

- Dalriada Executive – external affairs and business development (meets quarterly).
- Operations Executive – coordination of resources and internal operations (meets monthly).
- PPF/FAS Group – coordinates all PPF Assessment and FAS work (fortnightly conference call).
- Risk & Audit Committee – considers Group level risk and audit issues (meets quarterly).
- IT Group – drives IT strategy for the Group (meets quarterly).
- Investment Sub-Committee – considers investment strategic investment decisions / policy issues (meets quarterly).
- Irregular Schemes Sub-Committee – acts on the delegated authority of the Dalriada board with regard to each of the Irregular Schemes to which Dalriada has been appointed as an independent trustee by The Pensions Regulator, where The Pensions Regulator has concerns in relation to the management of the schemes (meets quarterly).

3 | Pension Trustee and Administration Services



3 Pension Trustee and Administration Services

Dalriada provides a range of pension related services, including pension administration and database management, operated within a quality controlled environment where it acts as a professional trustee. This report covers the controls in place for our Pensions Delivery Function, the controls in place for other services provided by Dalriada are covered in our AAF 02/07 report for the period 1 January 2020 to 31 December 2020.

In some circumstances, Dalriada may be appointed as trustee for a scheme where these services are provided by a third party administrator, and in certain cases Dalriada may elect to outsource some or all of these services in this way. The services provided by third party administrators are outside of the scope of this report although the third parties may prepare their own Assurance Report.

Our pension administration team 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.

Dalriada recognises that its administration service is the interface between a pension scheme and its members and 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 an accurate and 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 including Trusteeship, Fund Accounting 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 documented as a series of control documents available on our intranet site. Where relevant all documents are managed within our formal Information Security Management System ("ISMS"). Dalriada's ISMS is externally certified under ISO/IEC 27001:2013.

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 system implementation with version control.

All of our members of staff have access to a wide variety of technical information sources.

CHECKING

There are strict checking procedures for all calculations and correspondence with our co-trustees (where relevant), 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 out.

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 but 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 the SLAs have been met. This allows the Trustees to monitor the performance against the SLA.

ELECTRIC DOCUMENT AND TASK MANAGEMENT

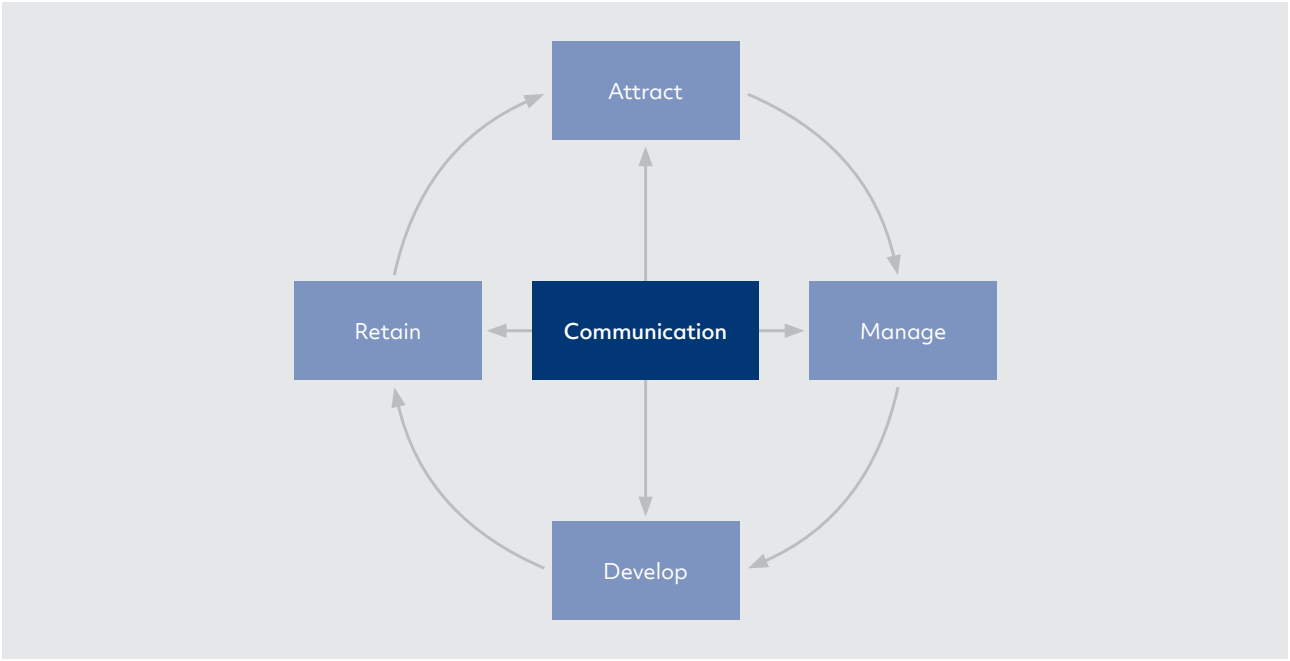
To underpin our workflow management system, we have implemented Microsoft SharePoint software enabling us to introduce comprehensive electronic document management. All correspondence for our clients is scanned and available for searching and retrieval. Our workflow system enables pensions administrators 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. Dalriada has also 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 02/07). The ISMS is subject to separate external audit for ISO 27001 purposes.

OUR EMPLOYEES

Our Company ethos is to provide worthwhile and interesting careers for all our employees. Our Human Resources team works in partnership with our Function Head Group to deliver the HR strategy of Attract, Manage, Develop, Retain and support the overall strategy of the Company.



- **Attract** - As a Company we recruit the highest calibre of staff 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 the annual appraisals are integrated with our salary and bonus system rewarding high performance against agreed objectives aligned with the needs of our business and our clients.
- **Develop** - We adopt a supported Learning and Development approach working with our employees through professional qualifications, formal study plans and mentoring, to enhance the capability of our employees and thus enhance our client service. All of our operational managers have been taken through management development training which has been developed specifically in relation 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 clearly defined and documented policies and procedures governing the services we provide which are clearly communicated to all relevant staff.
- 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 staff and relevant contractors.
- Compliance with our standards and relevant policies and procedures is regularly audited.

KNOWLEDGE MANAGEMENT

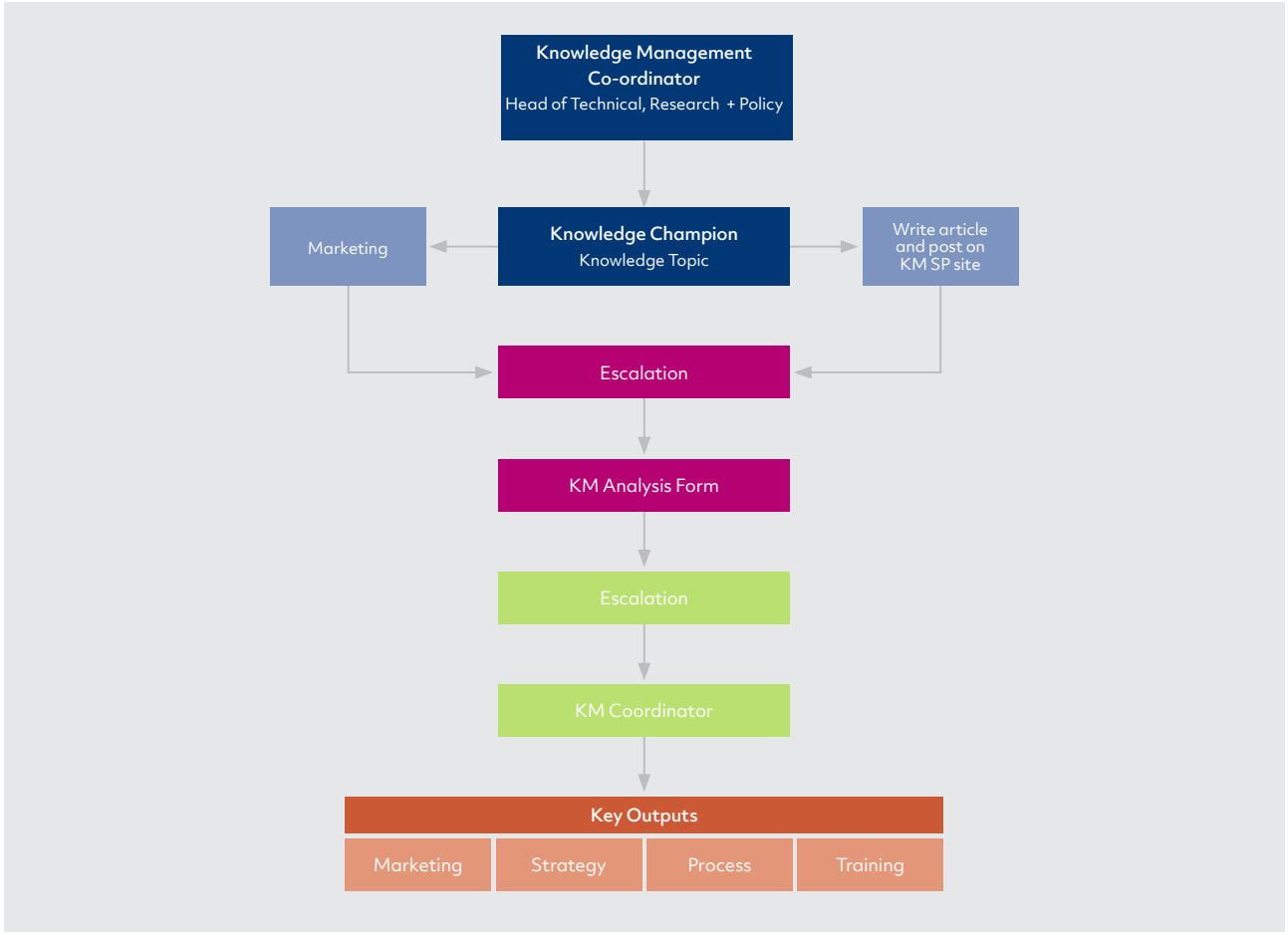
As part of our ongoing development of Knowledge Management, the Directors, in December 2019, recruited John Wilson, who has over 30 years' experience, as Head of Technical, Research and Policy. One of the responsibilities of this role is Knowledge Management Co-ordinator.

The Knowledge Management Co-ordinator ("KMCO") has responsibility for coordinating the Knowledge Management ("KM") process. This involves, in addition to production of KM output, reviewing the output produced by Knowledge 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 the KM information, as well as production and facilitator of information.

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

- Management and ownership of the KM piece across the business including a programme plan of projects, training and other activities to ensure control of delivery into the business.
- Understanding and 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 Champions or not.
- 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/clients internal and external.
- Meet with and report to the Risk & Audit Committee regularly, with appropriate updates when required to Practice and Function Heads Groups, as well as the Board of Directors.

The below diagram outlines our process.



We appoint Knowledge Subject Matter Champions who are experts in particular technical areas and develop the company and client understanding on key updates.

CULTURE

Our culture has a vital role to play in the delivery of our vision and our achievement of quality.

Our culture is embedded in everything we do and lived out by our employees. We have annual training days attended by all employees, where we outline strategy and focus on Group wide communication within an environment which encourages and allows open and honest feedback. We always benefit from a tremendous level of participation by employees on these days and value the input we receive from them.

Information Security

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

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

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

ISO 27001 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 Dalriada 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;
- 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 Dalriada Trustees Limited handles personal information in compliance with the General Data Protection Regulation ("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 'sensitive personal data'. We are named as a data controller under the register kept by the Information Commissioner in accordance with the GDPR.

Dalriada 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 Dalriada is 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 Dalriada 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 members of 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.

How our Communications with Trustees and Members Meet the GDPR Requirements

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 the personal data, and

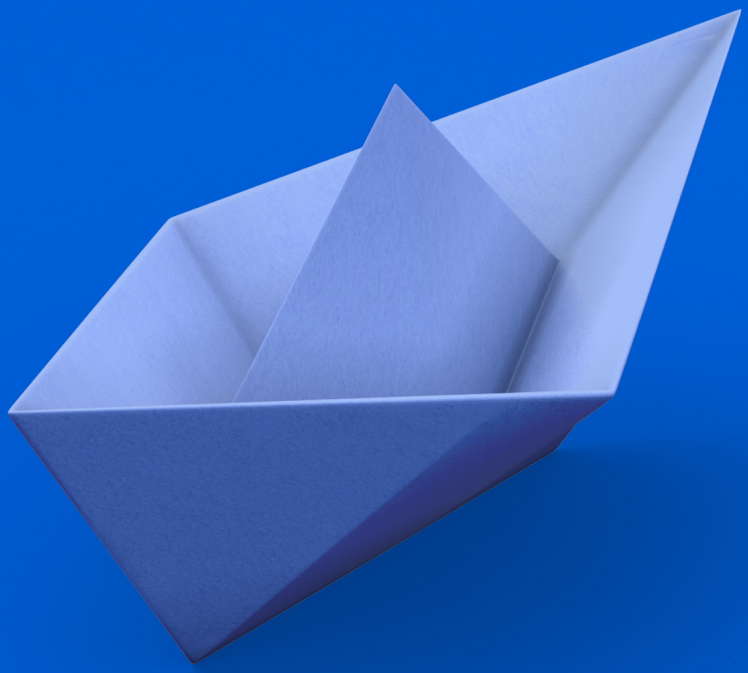
— the lawful basis for the processing. This would apply whether we collect the personal data directly from the individual, or if it is collected from another source.

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 papers like meeting packs, which avoids the need for storing and sharing of multiple hard copies of meeting packs.

4 | Risk Management



4 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 Information Security Focus Group ("ISFG") meets quarterly and analyses risk scenarios.

The business impact and consequences of each risk are assessed 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) the extent to which it is business critical rating, 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 countermeasures. The Risk Treatment Plans are escalated and formally approved where appropriate.

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

5 | Information Technology

5 Information Technology

Dalriada'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.

Dalriada has an in-house team of experts that manage and maintain Office 365 and Azure, this is complimented with a managed service provider offering.

Dalriada also utilises Mantle® an innovative web application provided by Dalriada'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

Dalriada has recently upgraded their 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.

SHAREPOINT

We use SharePoint Online as a central resource for document management and workflow. 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 with Dalriada simply consuming the service rather than maintaining it. This transfers the responsibility of 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.

Dalriada 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

Dalriada 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

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 is security measures are applied to all devices to ensure a device is compliant before it can access company data.

Dalriada can revoke any company data from any corporate device with immediate effect should the need arise.

All accounts are protected with Microsoft Multifactor Authentication ("MFA").

6 | Report from the Directors of Dalriada Trustees

6 Report from the Directors of Dalriada Trustees

As Directors of Dalriada Trustees Limited, we are responsible for the identification of control objectives relating to pension scheme transactions in the provision of pension administration services and the design, implementation and operation of the control procedures of Dalriada to provide reasonable assurance that the control objectives are achieved.

In carrying out those responsibilities we have regard not only to the interests of our pension scheme members, but also to the requirements of the business and the general effectiveness and efficiency of the relevant operations.

We have evaluated the effectiveness of Dalriada's control procedures having regard to the International Standard on Assurance Engagements 3402 ("ISAE 3402"), issued by the International Auditing and Assurance Standards Board, the Technical Release AAF 01/06 ("AAF 01/06"), issued by the Institute of Chartered Accountants in England and Wales, and the criteria for pension administration and pension database services. The control objectives identified include all of those listed in Appendices 1(c) and 1(g) of the ICAEW AAF 01/20.

We set out in this report a description of the relevant control objectives together with the related control procedures which were in operation during the year ended 31 December 2020 and confirm that:

- the report describes fairly the control objectives that relate to the control procedures referred to above, which were in place for the year ended 31 December 2020;
- the control procedures described were suitably designed throughout the year ended 31 December 2020 such that there is reasonable assurance that the specified control objectives would be achieved if the described control procedures were complied with satisfactorily; and
- the control procedures described were operating with sufficient effectiveness to provide reasonable assurance that the related control objectives were achieved during the year ended 31 December 2020.

Tom Lukic
Director
Signed on behalf of the Board of Directors
Dalriada Trustees Limited

Date: 26 February 2021

7 | Independent Assurance Report

7 Independent Assurance Report

RSM

Number One Lanyon Quay
Belfast
BT1 3LG

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

rsmuk.com

INDEPENDENT ASSURANCE REPORT ON INTERNAL CONTROLS OF DALRIADA TRUSTEES LIMITED

This report is made solely for the use of the directors, as a body, of Dalriada Trustees Limited ("the Organisation"), and solely for the purpose of reporting on the internal controls of the Organisation, in accordance with the terms of our engagement letter dated 20th October 2020 and attached as Appendix 1 to your report.

Use of 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 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.

This report is designed to meet the agreed requirements of the 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 Northern Ireland (UK) Limited for any purpose or in any context. Any party other than the 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 Northern Ireland (UK) Limited 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 report, in full only, to customers of the Organisation using the Organisation's pension administration services ("Customers") as defined in Appendix 1 to our engagement letter dated 20th October 2020, and to the auditors of such Customers, to enable Customers and their auditors to verify that a report by reporting accountants has been commissioned by the directors of the Organisation and issued in connection with the internal controls of the Organisation without assuming or accepting any responsibility or liability to them on our part.

Scope

We have been engaged to report on the Organisation's description of its pension administration services throughout the period 1st January 2020 to 31st December 2020 (the description), and on the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description.

Service Organisation's Responsibilities

The Organisation is responsible for:

- preparing the description and the accompanying assertion set out on page 24, including the completeness, accuracy, and method of presentation of the description and the assertion;
- providing the services covered by the description;
- specifying the criteria including the control objectives and stating them in the description;
- identifying the risks that threaten the achievement of the control objectives; and
- designing, implementing and effectively operating controls to achieve the related control objectives stated in the description.

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

Reporting Accountants' Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in that description. We conducted our engagement in accordance with International Standard on Assurance Engagements 3000 and 3402, and ICAEW Technical Release AAF 01/06. That standard and guidance require that we comply with ethical requirements and plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description, throughout the period 1st January 2020 to 31st December 2020.

Our work involved performing procedures to obtain evidence about the presentation of the description of the pension administration services and the design and operating effectiveness of those controls. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description.

Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related control objectives stated in the description were achieved.

An assurance engagement of this type also includes evaluating the overall presentation of the description and the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organisation and described at page 24.

Inherent Limitations

Our audit work on the financial statements of the Organisation is carried out in accordance with our statutory obligations and is subject to separate terms and conditions. This engagement will not be treated as having any effect on our separate duties and responsibilities as the Organisation's external auditors. Our audit report on the financial statements is made solely to the Organisation's members, as a body, in accordance with Chapter 3 of Part 16 of the Companies Act 2006. Our audit work has been undertaken so that we might state to the Organisation's members those matters we are required to state to them in an auditor's report and for no other purpose. To the fullest extent permitted by law, we do not accept or assume responsibility to anyone other than the Organisation and the

Organisation's members as a body, for our audit work, for our audit reports, or for the opinions we have formed.

To the fullest extent permitted by law we do not and will not, by virtue of our reports/confirmations or otherwise, assume or accept any duty of care or liability under this engagement to the Organisation or to any other party, whether in contract, negligence or otherwise in relation to our audits of the Organisation's financial statements.

The Organisation's description is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of the pension administration services that each individual customer may consider important in its own particular environment. Also, because of their nature, controls at a service organisation may not prevent or detect and correct all errors or omissions in processing or reporting transactions or identification of the function performed by the service organisation or system.

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

Respective responsibilities

Our responsibility is to form an independent conclusion, based on the work carried out in relation to the control procedures of Dalriada's pension administration services as described in the directors' report and report this to the directors of Dalriada.

OPINION

In our opinion, in all material respects, based on the criteria including specified control objectives described in the directors' assertion on page 24:

a) the description on pages 12 to 22 fairly presents the Pension Administration Services that were designed and implemented throughout the period from 1st January 2020 to 31st December 2020;

b) the controls related to the control objectives stated in the description on pages 30 to 33 were suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls operated effectively throughout the period from 1st January 2020 to 31st December 2020;

c) the controls that we tested were operating with sufficient effectiveness to provide reasonable assurance that the related control objectives stated in the description were achieved throughout the period 1st January 2020 to 31st December 2020.

Description of Tests and Controls

The specific controls tested and the nature, timing and results of those tests are detailed on pages 35 to 63.

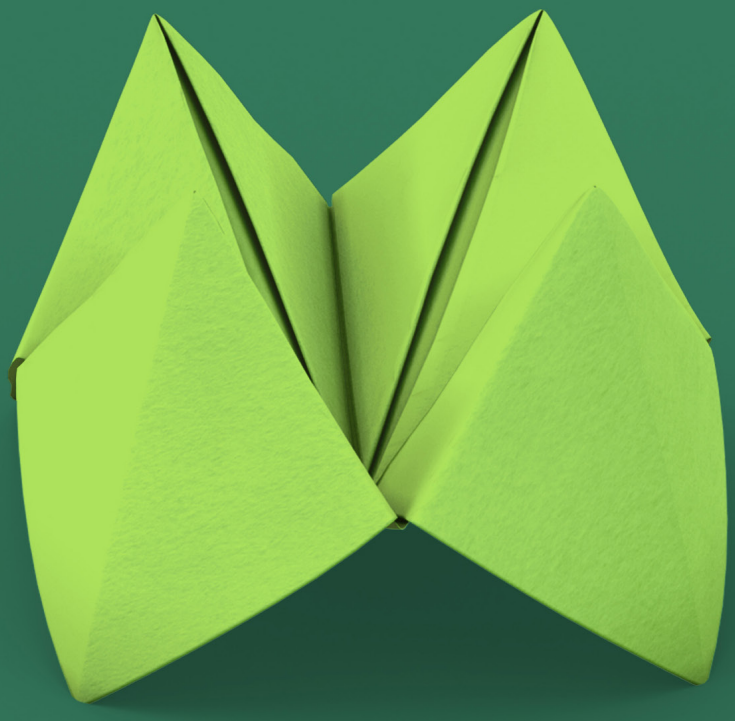
We have no responsibility to update this letter for events and circumstances occurring after the date of this letter.

RSM Northern Ireland (UK) Limited

RSM Northern Ireland (UK) Limited

26th February 2021

8 | Summary of Control Objectives



8 Summary of Control Objectives

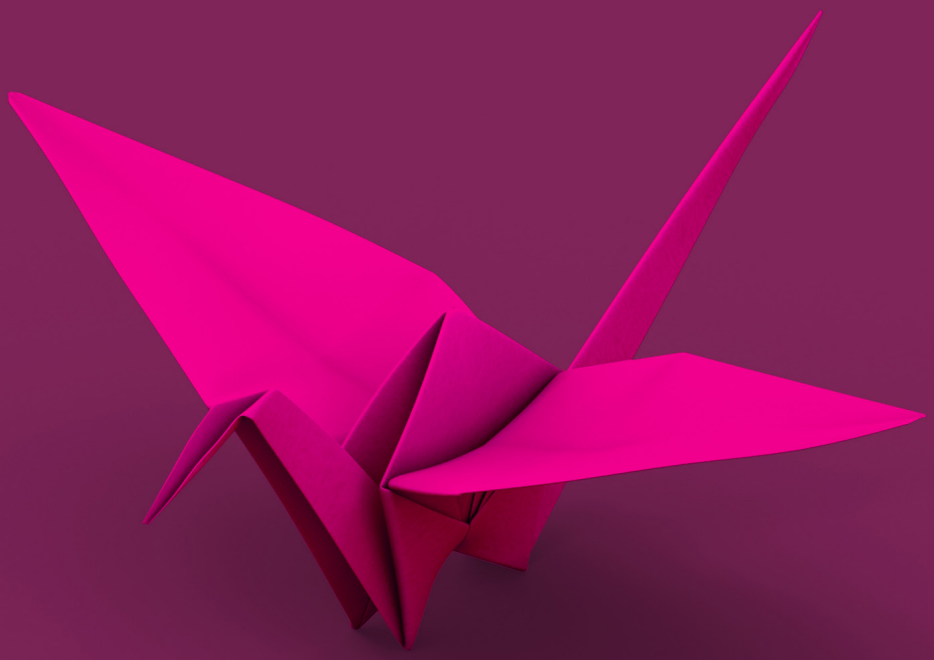
Control Objective	Audit Findings
1. Accepting Clients	
Accounts are set up and administered in accordance with the Schemes' Trust Deed and Rules, or Appointment Order from the Pensions Regulator ("TPR") and applicable regulations.	**No exceptions noted.**
The appropriate Deed of Appointment is executed by all parties, or Appointment Order from TPR is received 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. Authorisation 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.**
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.**
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.**

Control Objective	Audit Findings
4. Safeguarding Assets	
Member and scheme data is appropriately stored 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 (where Dalriada carry out the treasury function).	**No exceptions noted.**
Services provided to pension schemes are in line with agreed service levels.	**No exceptions noted.**
Transaction errors are rectified promptly and clients treated fairly.	**No exceptions noted.**
6. Reporting to Clients	
Periodic reports to co-Trustees and scheme sponsors, where applicable, are accurate and complete and provided within agreed timescales.	**No exceptions noted.**
Annual reports and accounts are prepared in accordance with applicable law and regulations.	**No exceptions noted.**
Information Technology	
7. Restricting Access to Systems and Data	
Physical access to computer networks, equipment, storage media and program documentation is restricted to authorised individuals.	**No exceptions noted.**
Logical access to computer systems, programs, master data, transaction data and parameters, including access by administrators to applications, databases, systems and networks, is restricted to authorised individuals via information security tools and techniques.	**No exceptions noted.**

Control Objective	Audit Findings
Segregation of incompatible duties is defined, implemented, and enforced by logical security controls in accordance with job roles.	**No exceptions noted.**
8. Providing integrity and resilience to the information processing environment, commensurate with the value of the information held, information processing performed and external threats	
IT processing is authorised and scheduled appropriately, and exceptions identified and resolved in a timely manner.	**No exceptions noted.**
Data transmissions between the service organisation and its counterparties are complete, accurate, timely and secure.	**No exceptions noted.**
Appropriate measures are implemented to counter the threat from malicious electronic attack (e.g. Firewalls, anti-virus etc.).	**No exceptions noted.**
The physical IT equipment is maintained in a controlled environment.	**No exceptions noted.**
9. Maintaining and developing systems hardware and software	
Development and implementation of new systems, applications and software, and changes to existing systems, applications, and software, are authorised, tested, approved, and implemented.	**No exceptions noted.**
Data migration or modification is authorised, tested, and once performed, reconciled back to the source data.	**No exceptions noted.**
10. Recovering from processing interruptions	
Data and systems are backed up regularly, retained offsite and regularly tested for recoverability.	**No exceptions noted.**
IT software and hardware issues are monitored and resolved in a timely manner.	**No exceptions noted.**
Business and information systems recovery plans are documented, approved, tested and maintained.	**No exceptions noted.**

Control Objective	Audit Findings
11. Monitoring Compliance	
Outsourced activities are properly managed and monitored.	**No exceptions noted.**

9 | Control Procedures and Audit Testing



9 Control Procedures and Audit Testing

Control Objective	Audit Findings
1. Accepting Clients	
On confirmation that Dalriada has been appointed by Deed of Appointment or by Order of TPR and will be providing administration services a New Client Implementation Document is prepared to act as a project planning document. 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.	Verified for a sample of new scheme acceptances during 2020 that the client Initial Take On Document, Pre-Appointment Conflict Consideration and Accepting Business Risk Management have been completed and signed off by both the client and the Dalriada Client Manager. **No exceptions noted.**
Only on receipt of a signed Deed of Appointment or Appointment Order from TPR, can the client be added to the workflow system such that people are able to record time against the client. Occasionally, due to time constraints, Dalriada may be required to carry out some work before it is possible to have the Deed signed. On receipt of a signed Deed or Order from TPR, this is scanned to SharePoint and tagged appropriately.	Verified for a sample of new scheme acceptances during 2020 that the appropriate Deed of Appointment or Appointment Order from TPR is correctly scanned and retained in SharePoint. **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 which are reviewed and signed off. Where appropriate, the Benefit Specification is reviewed and signed off by our co-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. The remaining control objectives assume that the relevant service is not outsourced to a third party.	Verified for a sample of client take-ons during 2020 that the Scheme Installation Checklist has been signed and filed, the Benefit Specification has been compiled from Scheme Rules and filed, that amendments over time have been reviewed and signed off by the client manager, and that the Benefit Specification has been signed by the trustees. Verified that data migration and reconciliation has been carried out for a sample of clients as well as a data audit to test the data quality standards. **No exceptions noted.**
Prior to commencement of administration services, the Pension database team's business analyst reconciles scheme data provided by the previous administrator to Dalriada's administration system, and raises any exceptions regarding missing or incorrect data with the client manager. Data is analysed using Dalriada's bespoke data audit software, which generates reports that identify any gaps or errors in the data received. Reports generated by the data audit, along with correspondence to resolve any data gaps or errors, are held on our document management system	Verified for a sample of new schemes that a data reconciliation / audit of the previous schemes data has been completed. **No exceptions noted.**

Control Objective	Audit Findings
Data is requested in all forms and any electronic data is imported onto Dalriada administration system 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 Dalriada cannot carry out some or all of the services they have been contracted to perform.	Verified for a sample of scheme accounts that membership statistics reconciliations are completed. **No exceptions noted.**
Scheme data reconciliations and correspondence relating to the follow up of any gaps or errors identified are verified by a member of the Pension database team as evidenced by the sign off on the scheme installation checklist. Copies of work relating to the installation are held on our document management system.	Verified for a sample of new schemes that a scheme installation checklist / plan has been completed and signed off as appropriate. **No exceptions noted.**
Wherever possible, Dalriada 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 for a sample of schemes that requests to view any previous administrator's specifications were made. **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 co-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 that the benefit specification was signed by the trustees and the legal advisor if applicable. **No exceptions noted.**
All documentation is scanned, tagged and filed in SharePoint, for ease of reference.	Verified for a sample of schemes that documentation is scanned and saved in SharePoint with the originals held in secure storage. **No exceptions noted.**

Control Objective	Audit Findings
2. Authorising and Processing Transactions Procedures	
Procedures are followed for banking cheques and electronic credits and contributions monitoring whereby all cheques received are logged and banked on the same day by the Business Support Team ("BST"). Electronic credits are logged by the accounts team. The paperwork accompanying the cheque/ electronic credit is passed to the accounts team who prepare a deposit form and update the transaction on QuickBooks and Xero to record receipt of the contributions. The deposit form is signed by the fund accountant/cashflow administrator and is filed.	Verified for a sample of receipts and cheques received throughout 2020 that they were logged and banked on the same day and that QuickBooks and Xero were updated in a timely manner. **No exceptions noted.**
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 for a sample of contributions that they were processed accurately and on a timely basis, and verified that outstanding contributions are followed up on a timely basis. Verified for a sample of errors and omissions that the appropriate notifications have been made to the administration manager, client manager and scheme actuary as appropriate. Confirmed through review of the Q2 and Q4 2020 Board minutes, that any breaches are included as part of the risk update to the Board. **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 will complete the appropriate checklist.	Verified for a sample of schemes that benefit calculations are accurately prepared on a timely basis, subjected to peer review and the appropriate checklist has been completed. **No exceptions noted.**

Control Objective	Audit Findings
Calculations are processed by an administrator in accordance with the scheme rules with reference to the scheme's benefit specification where appropriate. 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. 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.	Verified for a sample of scheme calculations that they have been processed in accordance with the scheme rules, have been signed off as reviewed by the client manager, actuarial calculation was completed by Mantle, checked by the Actuarial & Investment department and that the workflow checklist was completed within the service level agreement agreed with the client. **No exceptions noted.**
Procedures are followed for making cheques and electronic payments from the scheme bank account. 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 who are different from the requestor, processor and checker. Once a task has been completed it is closed off on the workflow system.	Verified for a sample of payments that they have been processed accurately and on a timely basis. All calculations were approved, the checklist prepared and approved for electronic payments, two relevant signatories completed on all cheques and the account balance updated. **No exceptions noted.**

Control Objective	Audit Findings
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. 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 Sage 50 Payroll Professional. Each payroll run for each client is reconciled by the payroll administrator for recorded changes against the previous payroll run. Each change and reconciliation is peer reviewed for accuracy. Reconciliations and payroll reports for each period are saved on our file management system SharePoint. The payment file is checked against the payroll data before being uploaded to the online banking facility.	Verified for a sample of payroll runs that they were processed accurately and in a timely manner, with evidence of reconciliation including to take account of any changes from previous month, payroll checklist completed and peer review of all processing. **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 calculated in accordance with the scheme rules. Recurring tasks are 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 reconciliations of payroll file against administration data have been undertaken and that all payrolls have been checked and approved for payment. Verified for a sample of monthly scheme payrolls that pension increases have been calculated in line with scheme rules, 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 Objective	Audit Findings
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. 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 for a sample of active schemes that a renewal checklist is completed, calculations peer reviewed and data reconciled prior to producing the member benefit statement. **No exceptions noted.**
Where applicable, 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 database team. On receipt of data a business analyst follows the scheme update checklist to load the data onto Dalriada's administration system. 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 peer reviewed and info relating to the change held on SharePoint. **No exceptions noted.**
Any changes to the scheme membership are recorded on our administration database 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. Changes can be made on receipt in writing from members. Ad-hoc checklists are completed and backing documentation is scanned and filed in the member's file. All changes are checked by another administrator. Following a new application, cessation of service, retirement, death or transfer of benefits the member's status is updated on our administration database. An approval workflow is run against a pdf copy of the member print for any status changes and the appropriate checklist is completed and checked by a senior administrator.	Verified for a sample of deaths, transfers and retirements that following receipt of all relevant information the checklist/workflow is updated, calculations completed, peer review undertaken and relevant letter sent to the client confirming all processed in a timely manner. **No exceptions noted.**

Control Objective	Audit Findings
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 a periodic report on membership is prepared with member numbers reconciliation included in the scheme accounts. Confirmed for the sample that any discrepancies had been resolved. **No exceptions noted.**
Receipt of any documentation from members is scanned and filed onto Mantle and or SharePoint, scheme correspondence is scanned and filed in SharePoint and checked by the administrator. Documentation for transfers out includes the discharge forms 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 co-trustee or company authorisation where required. Copies of documents are tagged and filed in SharePoint. Any original documents are returned to the member by recorded delivery.	Confirmed that signed scheme documentation is retained on SharePoint, all requested scheme information was made available and reviewed electronically on either SharePoint or Mantle systems. **No exceptions noted.**
The pension payroll service 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 service administrator immediately by the administrator.	Verified from correspondence with the pension payroll administrator 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 schemes that for any pensioner deaths a letter is issued to the payroll agent to advise them in a timely manner. **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. 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.	Verified for a sample of scheme bank accounts that monthly reconciliations are undertaken for each schemes cash book in a timely manner with appropriate segregation of duties and peer review procedures in place. **No exceptions noted.**

Control Objective	Audit Findings
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 30 days of receipt of the bank statement unless queries arise which causes a delay. Uncashed cheques are monitored by the treasury team and if more than one month old are notified to the scheme administrator.	Confirmed through review of the Xero accounting software, for a sample of bank reconciliations, they are completed on a monthly basis. The bank reconciliations are checked by the Fund Accountant and are noted within the Xero accounting system as reconciled when complete. Confirmed that there were no uncashed cheques at the time of our review and Dalriada is moving away from using cheques. Verified that a daily system report is run showing all bank deposits including cheques. Cheques are reviewed by the Finance team and any unknown cheques are recorded on a register. The unknown cheques are monitored by the Treasury team who notify the administrator and follow up accordingly until resolved. **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 report are filed in Xero/SharePoint and the paper copies of bank statements are filed with the other post items but in a separate folder.	Verified for a sample that outstanding lodgements are queried and cleared down. Confirmed that bank statements are filed with post items but in a separate folder in SharePoint. **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 our administration database. Any discrepancies are investigated and resolved.	Verified that a sample of scheme contributions were reconciled to the schedule of contributions and benefit payments to the member movement report. All contributions were received in accordance with Dalriada and scheme rules, therefore no discrepancies requiring investigation. **No exceptions noted.**
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 manager's transactions.	Verified for a sample of schemes that income, purchases and sales in the scheme cashbook were reconciled to the investment managers record of transactions. All contributions were received in accordance with Dalriada and scheme rules, therefore no discrepancies requiring investigation. **No exceptions noted.**

Control Objective	Audit Findings
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 and disclosure regulations.	Verified 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. 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. Monthly meetings were set for monitoring purposes. Verified for a sample of days that all journals are automatically posted into the Xero accounting software on a daily basis. Confirmed through review of the journal templates, the trial balance workings are included and a reconciliation is completed on the journals to ensure accuracy. Confirmed that all journals are reviewed as part of the external audited accounts. **No exceptions noted.**
4. Safeguarding assets	
Access to Dalriada networks and administration database is restricted to authorised individuals, who gain access with unique logins and passwords that are compliant with industry standards. Segregation of duties rules for pensions administrators are enforced by security profiles built into the administration system. Profiles are assigned to pensions administrators based on their roles and responsibilities. User access to the systems is reviewed on a regular basis.	Confirmed through review that a Physical and Environmental Security process (Version 17, dated 29/09/2020) is in place, is subject to review on an annual basis and clearly outlines the physical security controls for access to all office locations. Verified through review of a video taken during May 2020 showing access to the office and a live webcam video during audit fieldwork that a key fob is required to access both the main building and lift to the office floors. Both a key fob and physical key are required to access the two server rooms. Confirmed through review of the server room list of key holders that only staff listed are authorised to access the Server rooms. Reviewed a copy of the key register and confirmed that staff are required to sign in and sign out when they access the server rooms. **No exceptions noted.**

Control Objective	Audit Findings
All new staff complete an online data protection training course as part of their induction when they join the Company. Refresher training is given periodically as and when required. Staff sign a security and confidentiality policy, a copy of which is held on their HR record.	Confirmed through review that all devices have encryption and password security controls in place that can only be managed by the IT team with administrator rights. **No exceptions noted.** Verified for a sample of 10 new joiners that an Access NI check was completed and a non-disclosure agreement and Security and Confidentiality policy had been signed and retained on file prior to commencement of employment. Verified that mandatory training is completed for all new starts across 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.**

Control Objective	Audit Findings
Member data is held electronically on Mantle and scheme data is stored electronically in SharePoint. Any data/correspondence held in paper form pre-dating the introduction of SharePoint is securely held offsite. Dalriada outsource their off-site storage and archive facilities to a specialist organisation. In the event it is necessary to retrieve paper files, these are scanned to SharePoint and the originals returned to off-site storage. 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.	Verified that there is a clear desk policy in place and clearly outlined within the Business Support and Office Management Processes (version 19, dated 15/09/2020). The policy is subject to review on an annual basis and is communicated to all staff. We were shown videos, one recorded in May 2020 and a live webcam walkthrough at the time of the audit fieldwork confirming no staff were in the office due to the pandemic lockdown and that all desks were clear. Verified through review of a sample of three-monthly rotas that during lockdowns as a result of the Covid-19 pandemic, that the Business Support Team attend the office daily on a rota basis to answer calls, emails and scan all incoming mail to SharePoint. The calls answered by the team are documented on the rotas by the Business Support team member responsible. Confidential waste bins are located in the office to securely dispose of sensitive information. The majority of paper documentation is securely stored off site and is managed by Doxbond. All sensitive paper documentation on site are securely located in locked filing cabinets within the locked filing rooms which are only accessible by authorised staff with key fob and biometric key pad access. We were shown videos of the requirements for access to the filing room and the contents of the filing cabinets, recorded from May 2020 and a live webcam walkthrough at the time of our audit fieldwork.

Control Objective	Audit Findings
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.	Verified that a Business Continuity Process and Plan are in place and up to date. The BCP Plan was published on 14/01/2020 and is subject to review on an annual basis. Both documents clearly outline the mission critical activities and processes and procedures to counteract disruptions to business activity. Confirmed through review of outcomes that a Business Continuity Test was completed during March 2020. Furthermore, it was confirmed through review of documentary evidence that a Contingency Planning Group was set up in January 2020, to promote active collaboration between key stakeholders to minimise the potential impact of the Covid-19 pandemic. **No exceptions noted.**
Dalriada has obtained ISO27001:2013 (information security) accreditation.	Verified the re-accreditation for ISO 27001 for Dalriada Trustees in 26/09/2020. Verified the re-accreditation for ISO 27001 for Spence and Partners on 25/09/2020. Verified the re-accreditation for ISO 27001 for Mantle Hosting on 07/07/2020. The certificates are valid for a period of three years. **No exceptions noted.**

Control Objective	Audit Findings
When taking on the administration of the trust account, bank forms and required information is 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 schemes that for bank accounts opened during 2020 bank forms and mandates were completed, signed by the trustees and had been signed by authorised signatories prior to forwarding to the bank. **No exceptions noted.**
Cheques are banked on the day of receipt unless they are subject to query. 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.**
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.	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 staff.	Confirmed through review of a video taken during May 2020 documenting entry to the locked filing room that cheque books are securely stored within a locked filing cabinet in the filing room. The filing room is only accessible to authorised staff from the Business Support Team with a key fob and biometric scanner. **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 cash flow is carried out monthly or quarterly by the cash flow administrator, peer reviewed and client manager reviewed, checklist completed and the investment or dis-investment transaction confirmed. **No exceptions noted.**

Control Objective	Audit Findings
Scheme expenses are not processed unless authorised by the relevant authoriser 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 2020, authorisation is required by relevant authoriser prior to payment. Verified that invoices are signed by the authoriser and an email is retained on the system from the authoriser and attached to the payment information. **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 on the same day unless a query arises. A scanned copy of the latest Schedule of Contributions is held on SharePoint. The amounts due are entered on the contributions monitoring spread sheet and monitored. Any unusual differences are investigated. The contributions monitoring spread sheet is reviewed on 19th of each month and any outstanding contributions usually received by that date are followed up. The receipt of outstanding contributions is monitored. Any late contributions are notified to the client manager. They are recorded on the breaches log which is on the agenda at the quarterly board meetings.	Verified for a sample of contributions that they were processed accurately and on a timely basis, and verified that outstanding contributions are followed up on a timely basis. Verified that the Schedule of Contributions is held on SharePoint. Verified for a sample of errors and omissions that the appropriate notifications have been made to the administration manager, client manager and scheme actuary as appropriate. Confirmed through review of the Q2 and Q4 2020 Board minutes, that any breaches are included as part of the risk update to the Board. **No exceptions noted.**
Service level agreements ("SLAs") are reported to the trustees in Stewardship Reports. The administration team aim to carry out services and tasks accurately and efficiently and to meet SLAs.	Verified that for a sample of schemes SLAs are in place and the performance against SLAs have been reported to the trustees in the stewardship reports. **No exceptions noted.**

Control Objective	Audit Findings
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 for a sample of workflows that the internal deadlines had been set shorter than the statutory disclosure deadlines and therefore disclosure breaches should be avoided. Workflows in the Mantle system detail the number of days taken and the status of the workflow, highlighting when a task deadline is approaching. **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. Stewardship reports' contents and frequency 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 their performance.	Verified for a sample of workflows that the internal deadlines had been set shorter than the statutory disclosure deadlines and therefore disclosure breaches should be avoided. Workflows in the Mantle system detail the number of days taken and the status of the workflow, highlighting when a task deadline is approaching. **No exceptions noted.**
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 of Directors 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 implemented for the recording of all incident, omissions, regulatory and DPA breaches and training was provided for relevant staff during December 2020. Verified through review of a sample of errors, omissions and DPA breaches, they were appropriately recorded, with incident date, incident identification date, incident number, responsible party, incident details, locality, departmental area and resolution outlined. Confirmed through review of Q3 and Q4 2020 minutes for the ISFG, incident reporting is a standing agenda item and the status of all incidents recorded are discussed. Reviewed Q2 and Q3 2020 Board meeting minutes and confirmed that any potential financial implications are discussed. **No exceptions noted.**

Control Objective	Audit Findings
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 client manager. The reports contain membership details provided from our administration database 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 any co- Trustee and the sponsoring company, where applicable, as and when required.	Verified for a sample of schemes that the quarterly stewardship reports were prepared, checked by a supervisor to confirm the completeness and accuracy of member movements and reconciliations, and provided to the scheme trustees on a timely basis. **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 for a sample of schemes with active members that bulk member data updates and ad-hoc individual member updates are reconciled on a regular basis, personalised annual benefit statements are prepared, peer reviewed, agreed to the summary benefit schedule and sent to scheme members on a timely basis. **No exceptions noted.**
Annual reports and accounts are prepared using the accounts template which complies with the latest Statement of Recommended Practice ("SORP") for pension schemes. Any changes to the standard template are logged on a proposed amendment spread sheet. 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 that a standard reporting format was in place for the creation of annual reports and accounts. The Statement of Recommended Practice ("SORP") was used as the template 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. Monthly meetings were set for the purpose of monitoring delivery versus the statutory deadline. Verified that scheme accounts are published within the statutory 7-month reporting deadline. **No exceptions noted.**

Control Objective	Audit Findings
The draft report will be passed to the client manager for review.	Verified that the accounts once in a draft format, they were reviewed by another fund accountant to ensure they were in line with the requirements of SORP. **No exceptions noted.**
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 any such meeting a report is circulated to the consultancy team, if requested.	Verified that a deadline of five months is set for the signing of scheme accounts. Verified that monthly meetings were set for the purpose of monitoring delivery versus the statutory deadline and reports circulated to consultancy team when requested. **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'. All compliance breaches are notified to the board of Directors as part of the internal management information reporting process. The client manager should determine if a regulatory report is required.	Confirmed that procedures are in place to monitor tasks on the workflow system and corresponding statutory deadlines. Verified for a sample of breaches that they were recorded in the regulatory breaches log, had been brought to the attention of the client manager, scheme actuary and trustees. Confirmed through review of the Q2 and Q3 Risk and Audit Committee reports and corresponding minutes that a regulatory report is presented outlining all regulatory breaches for the period. Confirmed through review of Q2 and Q3 2020 Board minutes that the Board are notified of any compliance breaches. **No exceptions noted.**

Control Objective	Audit Findings
7. Restricting Access to Systems and Data	
The business operates across seven office sites, Belfast, Birmingham, Bristol, Glasgow, Leeds, London and Manchester. The Physical and Environmental Process (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. The primary IT infrastructure resides at a secure, ISO 27001 certified, world class, off-site data centre.	Verified through review of a video taken during May 2020 documenting entry to the office building that a key fob is required to access the communal areas of the building and lift to access the Belfast office floors. Both a key fob and physical key are required to access the server rooms. Confirmed only authorised staff have access. Reviewed the service room list of key holders and confirmed only authorised personnel have access to the two server rooms. Reviewed a copy of the key register and confirmed that staff are required to sign in and sign out when they access the server rooms. These are the same procedures and controls for other office locations. **No exceptions noted.**

Control Objective	Audit Findings
Dalriada's full environment is replicated continuously to a Disaster Recovery environment hosted in a ISO27001 certified, world class, off site data centre. This features dual authentication and biometric scanning as well as card key access control and CCTV coverage with digital recording and archiving. The Belfast office is manned by security during office hours and is locked outside office hours. Only staff who require access outside office hours are given keys as approved and issued by the Business Support team who maintain 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.	Confirmed through observation of the IT system that two geographically separate datacentres 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). Confirmed through observation of movements of data between Dalriada servers and the datacentres for the BCP/DR tests. Verified the active Pay-As-You-Go subscription for the use of the datacentres through screenshots. Verified through review of a video taken during May 2020 documenting entry to the office building 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. Confirmed that during the pandemic, the security desk is not manned, however the communal entrance is locked, can only be accessed by authorised key fobs and staff require prior authorisation from management prior to accessing the office. We were shown email requests and authorisation from senior management for specific members of staff to be allowed access to the office to complete certain tasks. Confirmed there is a process in place for accessing the office outside office hours and a Director will approve staff requiring access to the office if and when required.

Control Objective	Audit Findings
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 entry 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' books 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 there is a process in place to report the loss of a key fob to the Business Support Team. Lost fobs are deactivated and a new fob is assigned and activated. Verified evidence to confirm 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 review that visitors are required to sign in at the reception desk via tablet prior to accessing the office, are provided with an office pass and are signed out by a member of the Business Support Team. Confirmed that the system penetration test has been delayed until March 2021 due to the pandemic. The last penetration test and IT Guarded audit report was reviewed during the previous internal audit review and no exceptions were noted. Given the postponement of the penetration test during 2020 due to the ongoing Covid-19 pandemic, confirmed there is continual assessment of vulnerabilities and threats to IT assets by reviewing internal penetration monitoring logs and dashboards for 2020. Verified that a number of SOC reports have been completed for Microsoft Office 365 (dated 26/01/2021), Microsoft Azure Development Ops (dated 12/01/2021). Confirmed through review that a number of ISO, SOC and GRC reports have been completed during 2020 to ensure the validity and compliance of the IT controls in place. **No exceptions noted.**
Windows laptops are configured by an automated build to have password protection and data encryption is enforced. Encryption for Windows laptops is managed via InTune as the Bitlocker key for the internal hard drive synchronises with the InTune entry for each Windows Laptop. When MacBook's are set up by IT Support the MacBook is encrypted with FileVault encryption and a password is set for the user and user is then asked to change this during first use. Access Control Process (Process 9).	Confirmed through review that all devices have encryption and password security controls in place that can only be managed by the IT team with administrator rights. **No exceptions noted.**

Control Objective	Audit Findings
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. An Information Security Focus Group manage all security weaknesses and vulnerabilities and meet 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. Documentation in paper form is stored off-site in a 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.	Verified there is a clear desk policy in place, is subject to review on an annual basis and is communicated to all staff. Confirmed through observation of the daily rotas for the Business Support Team that a nightly sweep of each office is completed at the end of the working day by the team to ensure all documentation has been secured, which has continued during the pandemic. Verified through a virtual walk around via live webcam during audit fieldwork of the office that all desks were clear. Verified that security training and awareness sessions are run periodically for all staff. Verified that during 2020, staff received both Cyber Security and Incident Awareness training. Verified that confidential waste bins are located in each office location to securely dispose of sensitive information. Verified through review of a sample of meeting minutes for Q2 and Q3 2020 that an Information Security Focus Group (IFSG) is in place and potential security weaknesses or vulnerabilities are discussed. The majority of paper documentation is securely stored off site and is managed by Doxbond. All sensitive paper documentation on site is securely located within locked filing cabinets in the locked filing rooms which is only accessible by Business Support Team staff with fob and biometric key pad access. This was confirmed via the live webcam walkaround as part of audit fieldwork and also in the video from May 2020. **No exceptions noted.**

Control Objective	Audit Findings
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 five leavers that the IT checklist was completed confirming all access rights were disabled and any IT assets e.g. Laptop, mobile phone, keys or fobs were returned and codes changed. The dates of the checklist completion and return of IT equipment was in line with the leaving date of all employees. Verified for a sample of ten new joiners the IT equipment and date allocated were recorded and in agreement with the start date of employment in all instances. **No exceptions noted.**
All access to computer equipment and systems is protected by passwords. Passwords expire after 42 days and users are prompted to change them. 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 (Process 9). All data must be stored on the corporate network and data is permitted on corporate owned assets that have been registered within the MDM solution.	Confirmed through review that all access to computer equipment and systems is protected by passwords. Passwords are required to be updated on a regular basis and cannot be simplistic in detail. Confirmed through review of the Security and Confidentiality Policy that passwords are required to be complex and at least 15 characters in length. **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 based upon their job function. Only authorised members of the IT Department can amend an individual's permissions. 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 authorised members of the IT Department. (Access Control Process 9).	Confirmed that only IT administrators can change access permissions. Confirmed through observation that multi-factor authentication is used to access data remotely. Verified for a sample of employees that user access for change of role required line manager authorisation prior to user access amendments by IT. **No exceptions noted.**

Control Objective	Audit Findings
8. Providing integrity and resilience to the information processing environment, commensurate with the value of the information held, information processing performed and external threats.	
Access to the administration system is controlled by windows authentication or two factor authentication on the relevant web browser. 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. 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.	Confirmed through observation that multi-factor authentication is used to access data remotely. Verified that different levels of security profiles are built into the administration system restricting unauthorised access. Confirmed that an audit trail history of changes to data is in place and cannot be deleted or cleared. Profiles are reviewed on a quarterly basis by the staff member's manager and are reviewed and amended by IT when a staff member changes roles or leaves the company. **No exceptions noted.**
All IT processing is carried out on laptops and desktop PCs in real time.	Observed a visual timeline of online processing activity by users and confirmed that all processing is carried out in real time. **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 based upon their job function. Only authorised members of the IT Department can amend an individual's permissions. 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 authorised members of the IT Department. (Access Control Process 9).	Confirmed that only IT administrators can change access permissions. Confirmed through observation that multi-factor authentication is used to access data remotely. Verified for a sample of employees that user access for change of role required line manager authorisation prior to user access amendments by IT. **No exceptions noted.**

Control Objective	Audit Findings
Dalriada 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.	Confirmed that SharePoint secure portal is used for the sharing of information externally where user access rights are confirmed. Confirmed through observation that multi-factor authentication is used to access data remotely. **No exceptions noted.**
All external access to the network is managed internally by the Chief Infrastructure Architect. Remote access set up is authorised by the IT Department and connections can only be made through Citrix Secure Desktop Software. The company contracts WaveNet to host a Firewall within its datacentre to control port access both in and out of the business. All email traffic is routed by a third party, Mimecast, who filter out any email threats i.e. viruses/spyware & inappropriate content.	Confirmed that all network access is required to be authorised by IT. Confirmed through observation that Windows Defender software is used to provide anti-virus protection. Confirmed through observation that Mimecast is used to monitor email traffic and remove threats. Confirmed through observation that Wavenet is used to provide firewall protection.
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.	Confirmed through observation that intrusion detection is in place. Verified the functionally of the software for a sample of two instances where the threat detection software had identified a potentially malicious URL link accessed in error by a staff member. The malicious URL was blocked and the IT desk alerted, who were then able to investigate the threat. **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.	There were no data migration projects to test during the year. Verified that appropriate procedures were in place to ensure accuracy and completeness. **No exceptions noted.**

Control Objective	Audit Findings
Any changes to existing, or the implementation of new, infrastructure and systems follows the Operational Change Control process outlined in Operations Security (Process 12). A major change will typically be a planned implementation and this will be discussed at quarterly meetings or ad hoc as required. When a major change is required business impact is reviewed and formal sign off and authorisation fob is required. (Operations Security Process 12)	Confirmed that an internal change log is maintained within the IT Service Desk as per the change management procedures. Confirmed approvals must be obtained by two signatories separate from the original requestor. Verified the records in line with procedures for two changes carried out by Internal IT in 2020 and confirmed approvals for each change. **No exceptions noted.**
Dalriada has also adopted an effective Information 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 HTG and the Internal IT Department are the only authorised individuals that can perform installations or upgrades. Any maintenance is performed by authorised representatives from by the Chief Infrastructure Architect is given to staff members of any downtime to the network that is required for the maintenance of software	Verified the records in line with procedures for two changes carried out by Internal IT in 2020 and the change records contained all necessary information and appropriate authorisation. Confirmed that there is an automatic control in place for application updates for Apple Macs and Windows. 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. Verified that a number of SOC reports have been completed for Microsoft Office 365 (dated 26/01/2021), Microsoft Azure Development Ops (dated 12/01/2021). Confirmed through review that a number of ISO, SOC and GRC reports have been completed during 2020 to ensure the validity and compliance of the IT controls in place. Confirmed that only authorised individuals can complete IT updates and maintenance. Confirmed through review of the records for two changes carried out by Internal IT in 2020 and verified the potential impact, roll out plan, back out plan and testing were recorded. Any potential risks are recorded by the IFSG team and the risk register is updated accordingly for ongoing monitoring. **No exceptions noted.**

Control Objective	Audit Findings
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.	Confirmed through observation that Windows Defender software is used to provide anti-virus protection. Confirmed through observation that Mimecast is used to monitor email traffic and remove threats. Confirmed through observation that Wavenet is used to provide firewall protection. Confirmed through observation that intrusion detection is in place. Verified the functionally of the software for a sample of two instances where the threat detection software had identified a potentially malicious URL link accessed in error by a staff member. The malicious URL was blocked, and the IT desk alerted who were then able to investigate the threat. **No exceptions noted.**
Azure Patch Management – monthly updates. Windows updates are rolled out monthly to all computers on the network. Citrix is patched on a quarterly basis with the exception of security and critical patches which are deployed within 10 working days of release. Development of systems is facilitated by an appropriate rollback strategy.	Verified that patch updates are completed on a monthly basis. Confirmed Windows and Apple updates are driven by the relevant compliance policies. The updates are automatic and system functionality is restricted if the user does not perform the update after two updates have been issued. **No exceptions noted.**
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.	There were no data migration projects to test during the year. Verified that appropriate procedures were in place to ensure accuracy and completeness. **No exceptions noted.**

Control Objective	Audit Findings
10. Recovering from Processing Interruptions	
Dalriada 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. Dalriada uses Azure Site Recovery for Disaster recovery services. **Backup and Restore Technology** All servers in Azure are backed up on a daily basis at 23:30 UTC. Recovery snapshots are held for 2 days and daily backups are retained for 30 days. **Replication and Recovery Technology** Dalriada utilises Azure Site Recovery to replicated data between Azure datacentres (DC). The primary Azure DC is UK South and DR DC is UK West. Recovery Point Objective ("RPO") is under 1 hour. Recovery Time Objectives ("RTO") of under 4 hours for the entire virtual estate.	Confirmed through observation that two geographically separate datacentres are used to host the services to provide additional resilience. A replica of the primary data centre (UK South) is in place (UK West) and is used in the event of disaster recovery. Confirmed through observation of movements of data between Dalriada servers and the datacentres for the BCP/DR tests. Confirmed that Azure Site Recovery is in place which enables automatic data recovery. Verified through review of results that disaster recovery testing of the IT infrastructure is completed on a 90-day cycle and is in line with BCP plan. Confirmed a daily back up process is in place and there is a retention of 30 days maintained with the backup vaults. Confirmed failover tests of Azure (UK South) to Azure (UK West) have been conducted in 2020 where recovery was 3 minutes achieving a Recovery Point Objective ("RPO") of 1 hour. **No exceptions noted.**

Control Objective	Audit Findings
The Business Continuity Plan ("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, Dalriada third party resourcing, information / data hard copy and facilities) have also been included. 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 Dalriada third party resources are included in this command structure (Business Continuity Management Process (Process 17); Business Continuity Plan, Dalriada BCP Testing Schedule and results 2011 to 2020). 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.	Confirmed through review that a copy of the Group Business Continuity Plan (dated 14/01/2021 version 36.0) 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. Confirmed through review of results that a BCP test was completed during early 2020. **No exceptions noted.** Confirmed through review of a copy of the Group Business Continuity Plan (dated 14/01/2021 version 36.0) that a command structure is in place with roles and responsibilities for Gold and Silver team members clearly outlined and allocated. **No exceptions noted.** Confirmed that copies of the BCP are held securely offsite. Verified that the Business Continuity Plan is subject to review on an annual basis and a BCP test was completed during early 2020. **No exceptions noted.**

Control Objective	Audit Findings
(Organisation of Information Security Process 6) Dalriada 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.	Confirmed through observation that two geographically separate datacentres 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). The failover test was last completed on 21st January 2021. **No exceptions noted.**
11. Monitoring Compliance	
Dalriada ultilises Log Analytics and ControlUp to monitor service health. Azure Dalriada outsources Citrix managing and monitoring to HTG. 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 3rd party audits conducted on a regular basis. Dalriada also employ 3rd party penetration and security experts IT Guarded to audit the network infrastructure annually. (Process 6 Organisation of Information Security and Process 10 Cryptography).	Confirmed that an IT ticketing system is used internally for IT service needs. Confirmed that a quarterly IT subcommittee meeting is held following an ad-hoc agenda with any major issues being escalated to the Board meetings. Verified for a sample of subcommittee minutes for Q2 and Q3 2020, that any information security issues followed the appropriate procedure. Verified that ISO27001:2013 and ISO9001:2015 audits were completed during 2020. Verified for a sample of third parties, that service level agreements are in place and third-party performance is subject to review on an ongoing basis. The Penetration tests are planned for March 2021 and have been delayed due to the pandemic. The last penetration test and IT Guarded audit report was reviewed during the previous internal audit review and no exceptions were noted. **No exceptions noted.**

Appendices

1 Appendices: Letter of Engagement

Our ref: IRM

Strictly Private & Confidential

The Directors
Dalriada Trustees Limited
Linen Loft
27-37 Adelaide Street
Belfast
United Kingdom
BT2 8FE

20th October 2020

To the directors of Dalriada Trustees 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 Technical Release AAF 01/06 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 May 2018.

RESPONSIBILITIES OF DIRECTORS AND REPORTING ACCOUNTANTS

The board of directors ('the Directors') of Dalriada Trustees Limited in relation to which the reporting accountants' assurance report is to be provided ('the Organisation') are and shall be responsible for the design, implementation and operation of control procedures that provide an adequate level of control over customers' assets and related transactions. The Directors' responsibilities are and shall include:

- acceptance of responsibility for internal controls;
- evaluation of the effectiveness of the service organisation's control procedures using suitable criteria;
- supporting their evaluation with sufficient evidence, including documentation; and
- providing a written report ('Directors' Report') of the effectiveness of the service organisation's internal controls for the relevant financial period.

In drafting this report the Directors have regard to, as a minimum, the criteria specified within the Technical Release AAF 01/06 issued by the Institute of Chartered Accountants in England and Wales ('the Institute') but they may add to these to the extent that this is considered appropriate in order to meet customers' expectations.

RESPONSIBILITIES OF REPORTING ACCOUNTANTS

It is our responsibility to form an independent conclusion, based on the work carried out in relation to the control procedures of the Organisation's administration, accounting and information technology functions carried out at the Belfast business unit of the Organisation as described in the Directors' Report and report this to the Directors.

SCOPE OF THE REPORTING ACCOUNTANTS' WORK

We conduct our work in accordance with the procedures set out in AAF 01/06, issued by the Institute. Our work will include enquiries of management, together with tests of certain specific control procedures which will be set out in an appendix to our report.

In reaching our conclusion, the criteria against which the control procedures are to be evaluated are the internal control objectives developed for service organisations as set out within the AAF 01/06 issued by the Institute.

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 the Directors in relation to matters on which independent corroboration is not available. We shall seek confirmation from the Directors 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 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.

INHERENT LIMITATIONS

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

USE OF OUR REPORT

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

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

Our report will be issued on the basis that it must not be recited or referred to or disclosed, in whole or in part, in any other document or to any other party, without the express prior written permission of the reporting accountants. We permit the disclosure of our report, in full only, to customers using the Organisation's services and to the auditors of such Customers, to enable Customers and their auditors to verify that a report by reporting accountants has been commissioned by the Directors of the Organisation and issued in connection with the internal controls of the Organisation without assuming or accepting any responsibility or liability to them on our part.

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

We will, exceptionally, agree to permit the disclosure of our Report on the Organisation's website, subject to, prior to this, us agreeing with you the wording of the introduction to the Report on your website. In addition this permission is granted only if the Report is published in full, to customers and potential customers of the Organisation using the Organisation's services ('Customers') and to the auditors of such Customers, to enable Customers and their auditors to verify that a report by reporting accountants has been commissioned by the Directors of the Organisation and issued in connection with the internal controls of the Organisation without assuming or accepting any responsibility or liability to them on our part.

Our Report must not be relied upon by Customers, their auditors or any other third party (together 'Third Parties') for any purpose whatsoever. RSM Northern Ireland (UK) Limited 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 our Report, they will do so at their own risk.

Our 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 Organisation agrees to indemnify and hold harmless RSM Northern Ireland (UK) Limited and its partners and staff against all actions, proceedings and claims brought or threatened against RSM Northern Ireland (UK) Limited or against any of its partners and staff by any persons other than the Directors as a body and the 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 Northern Ireland (UK) Limited's work under this engagement letter.

AGREEMENT OF TERMS

We shall be grateful if you will confirm in writing your agreement to these terms by signing and returning the enclosed copy of this letter, in the prepaid envelope provided, or let us know if the services covered are not in accordance with your understanding of the assignment to be carried out under the terms of this engagement.

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 Northern Ireland (UK) Limited

RSM NORTHERN IRELAND (UK) LIMITED

Encs. Terms and Conditions of Business dated May 2018

Contents noted and agreed for and on behalf of Dalriada Trustees Limited

Signed ..... Date 21 October 2020

AUTHORISED SIGNATORY

Dalriada. A better way

Belfast

Linen Loft
27-37 Adelaide Street
Belfast
BT2 8FE

Birmingham

Edmund House
12-22 Newhall Street
Birmingham
B3 3AS

Bristol

Castlemead
Lower Castle Street
Bristol
BS1 3AG

Glasgow

The Culzean Building
36 Renfield Street
Glasgow
G2 1LU

Leeds

Princes Exchange
Princes Square
Leeds
LS1 4HY

London

46 New Broad Street
London
EC2M 1JH

Manchester

82 King Street
Manchester
M2 4WQ