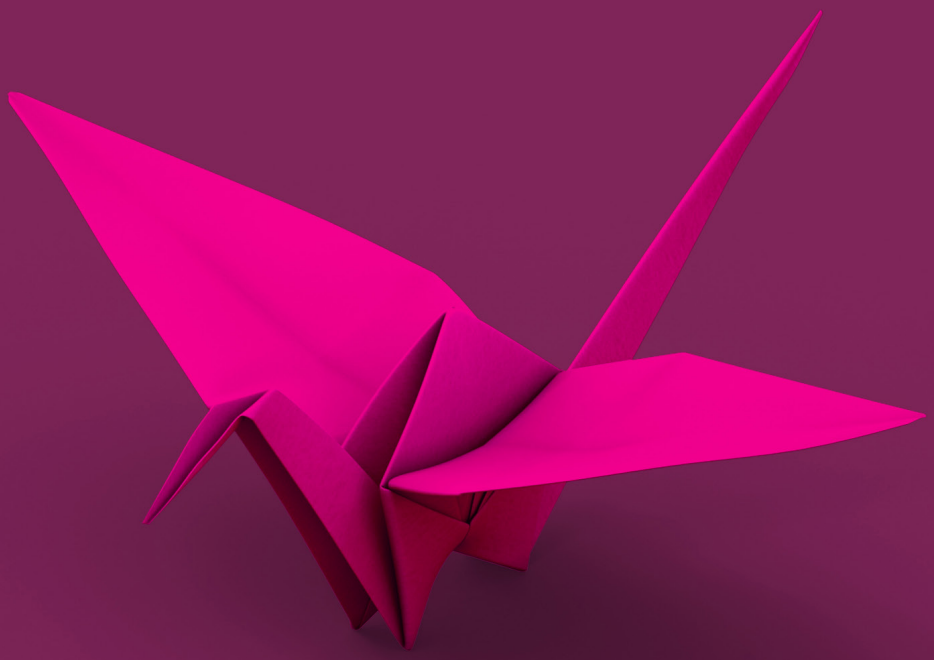
Assurance Report on Internal Controls

(AAF 02/07 and ISAE 3000)

For the period 1 January to
31 December 2021



Dalriada.
A better way

Statement of Reporting Accountants

RSM UK Risk Assurance Services LLP

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

Statement of Reporting Accountants

Our report as set out on page 2, has been prepared solely in accordance with the terms of engagement agreed by the Directors of Dalriada Trustees Limited with RSM UK Risk Assurance Services LLP and for the confidential use of Dalriada Trustees Limited ("Dalriada or 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 reason 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 and potential Customers, their auditors and any other third party (together "Third Parties") for any purpose whatsoever. RSM UK Risk Assurance Services LLP neither owes or 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.

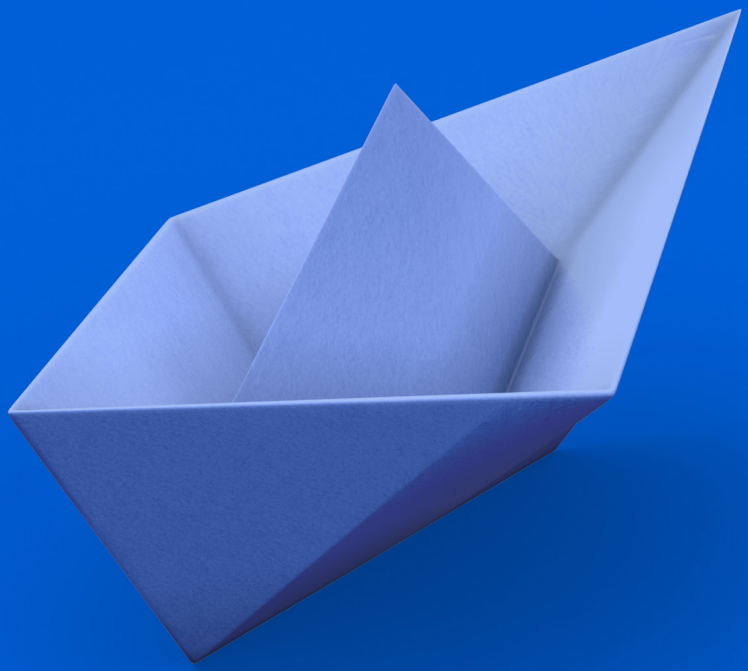
RSM UK Risk Assurance Services LLP

RSM UK Risk Assurance Services LLP

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

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 2021 and has been prepared in accordance with the Technical Release AAF 02/07 and AAF 05/20 "A Framework for Assurance Reports on Third Party Operations and Master Trusts", published by the Institute of Chartered Accountants in England and Wales ("the ICAEW") which also covers the one defined contribution master trust of which Dalriada is a trustee. As the control objectives are consistent with The International Standard on Assurance Engagements ("ISAE") 3000, 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 51. These measures have been audited and reported upon by RSM UK Risk Assurance Services LLP. This is the fifth such report we have published.

Dalriada is a privately owned UK company that acts as a professional trustee to UK occupational pension schemes. Our organisation is managed by eight Directors who supervise the activities of a number of highly experienced trustees, consultants, 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 trustee, 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 Trustee and Support Services Panel in 2020, offering specialist trustee services to schemes in a PPF assessment period. This replaced the PPF Trustee Advisory Panel, originally launched in 2013, where Dalriada had been on the panel since its inception. 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 2022.

SINCE **2003**

7 OFFICES

FIRST TRUSTEE FIRM IN THE UK TO SIGN PRI

300 SCHEMES MANAGED

48 ACCREDITED TRUSTEES

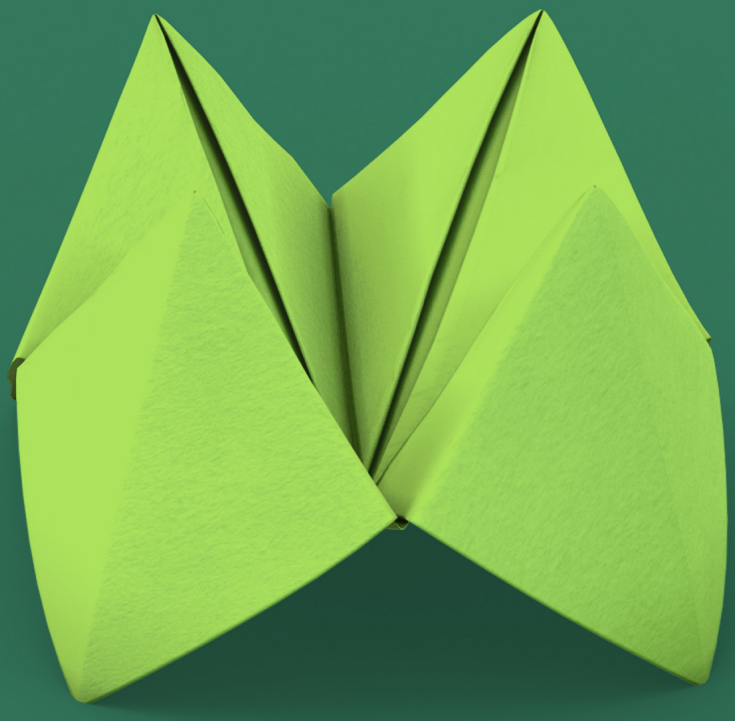
£11m TURNOVER 2020/2021

FROM **<£5M TO £20BN** CLIENT'S SCHEMES BY ASSET SIZE

<100 TO >1.5M MEMBERS IN SMALLEST TO LARGEST SCHEME

AAF 01/20, 02/07, ISO 27001 AND **ISO 9001** CERTIFIED

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 and with master trust strategists and funders 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.

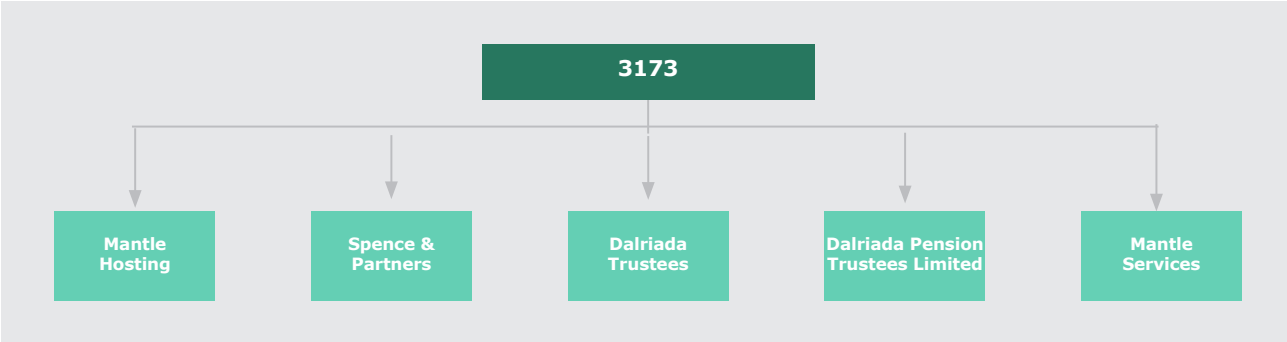
Dalriada applies process and technology to deliver more efficient and better service to our members. We work closely with partners committed to the use of Financial Technology ("Fintech") to develop online access for members, where possible and where this is their preference, timely reporting and best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

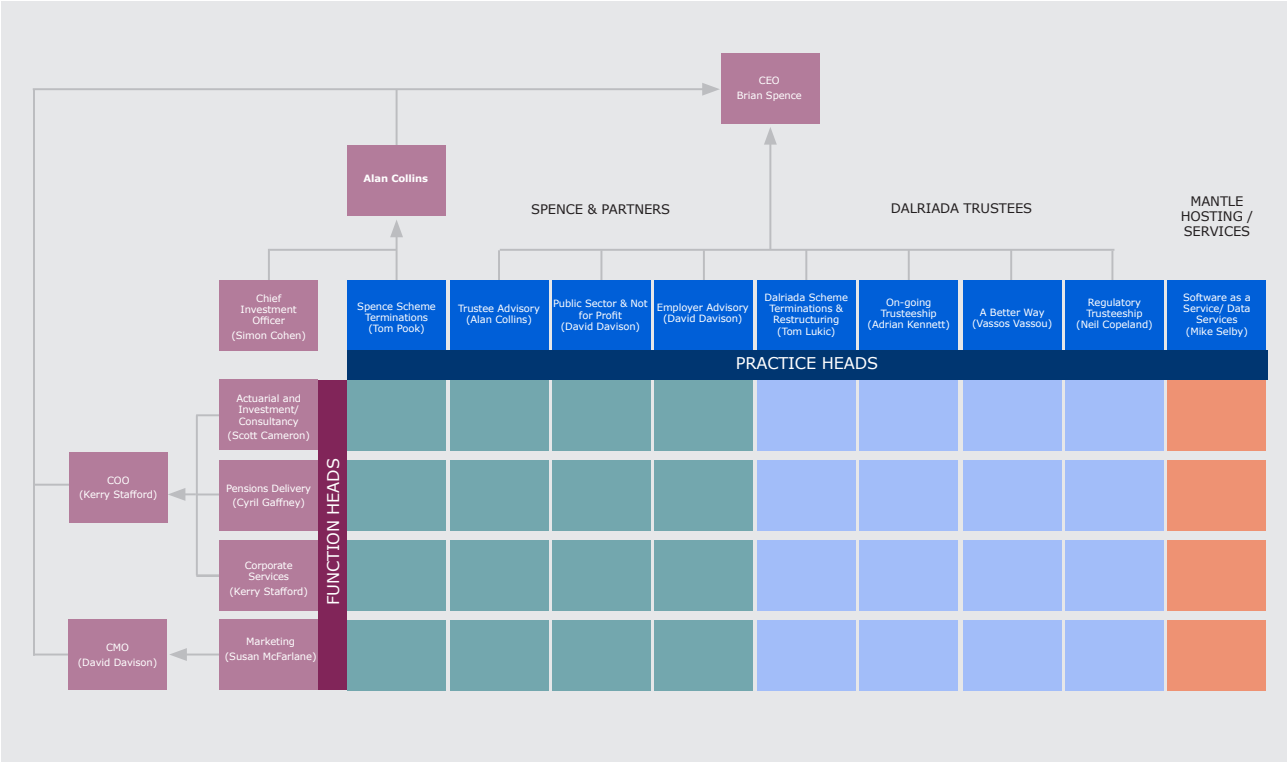
Our clients are based throughout the UK and Ireland and are serviced from our offices in Belfast, Birmingham, Bristol, Glasgow, Leeds, London, and Manchester.

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 actuaries, administrators, consultants, covenant advisors, investment and legal, pension database experts, pension fund accountants and project managers. The Group structure provides a flexibility which allows us to effectively manage resource levels to match variable workflows from clients, ensuring a consistency of service.

Our 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 businesses as a whole, and practice areas as required. The most relevant Functions for this report are our Consultancy and Pensions Delivery functions.

The role of the 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.

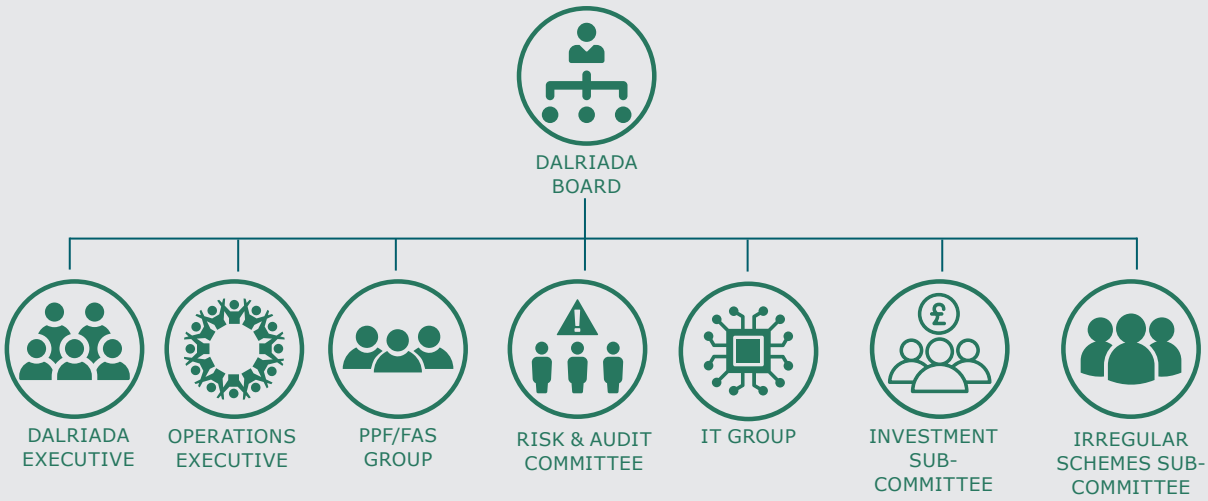
The separation between our Functions is not hard and fast. Although staff members are primarily associated with one Function, they can potentially perform a role in more than one Function, because we deliberately train staff to develop multiple skills.

In addition to the direct client servicing functions our Corporate Services Function contains internal finance, IT, 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. Our 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 Services

3 Pension Trustee Services

Dalriada provides a range of pension related services, operated within a quality controlled environment where it acts as a professional trustee.

The schemes that we deal with range widely in size of funds and membership, benefit structure, investment strategy, strength of employer covenant, funding levels and other technical complexities. Our trustee representatives have the ability to handle any scheme or situation that might be encountered.

We place great importance on ensuring that trustee decisions are well considered and robust. Our trustee representatives work with a highly skilled, experienced and enthusiastic team of support staff.

Dalriada offers a range of services tailored to the specific requirements of each scheme, including:

On occasions and where appropriate, Dalriada may elect to outsource certain services to a third party service provider. Where advisory services are required (for example administration services, actuarial, investment, legal, covenant) these are obtained by instructing a third party firm.

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. The controls in place for our Pension Delivery Function, which incorporates pension administration and pension delivery services, are covered in the AAF 01/20 report for the period 1 January 2021 to 31 December 2021.

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 and Pensions Delivery Functions), who manage the resources and day-to-day delivery of services.

PROCEDURES

Our procedures are owned by the relevant Function Head and evidenced in a series of control documents available on our intranet site. Where relevant, all documents are managed through our formal Information Security Management System (ISMS). Dalriada's ISMS is externally certified under ISO/IEC 27001:2013.

CONTENT MANAGEMENT

All procedures, documents, records and information are managed within an extensively developed SharePoint system implementation with version control, document creation and approval workflows.

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

CHECKING

There are strict checking procedures for all calculations and correspondence with each scheme's sponsoring employer, our co-trustees (where relevant), members and third parties, including regulatory bodies.

Checklists are completed to ensure that all the required steps are followed. All calculations are peer reviewed by a suitably qualified and experienced person (the checker), along with the checklist to ensure there are no errors or omissions.

All approval workflows for calculations and correspondence are held electronically in SharePoint.

ELECTRONIC DOCUMENT AND TASK MANAGEMENT

To underpin our workflow management system, we have implemented Microsoft SharePoint software enabling us to introduce comprehensive electronic document management. All non-member specific correspondence for our clients is scanned and available for searching and retrieval. SharePoint is also integrated with our bespoke workflow and time recording software, which enables trustee representatives 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. A number of scheme level activities are also monitored through our Client Relationship Management system.

Where Dalriada provides administration services, all member specific correspondence and workflow information is stored within Mantle, the administration software system. For those schemes, the trustee representative has access to Mantle and can monitor progress and performance of administration activity.

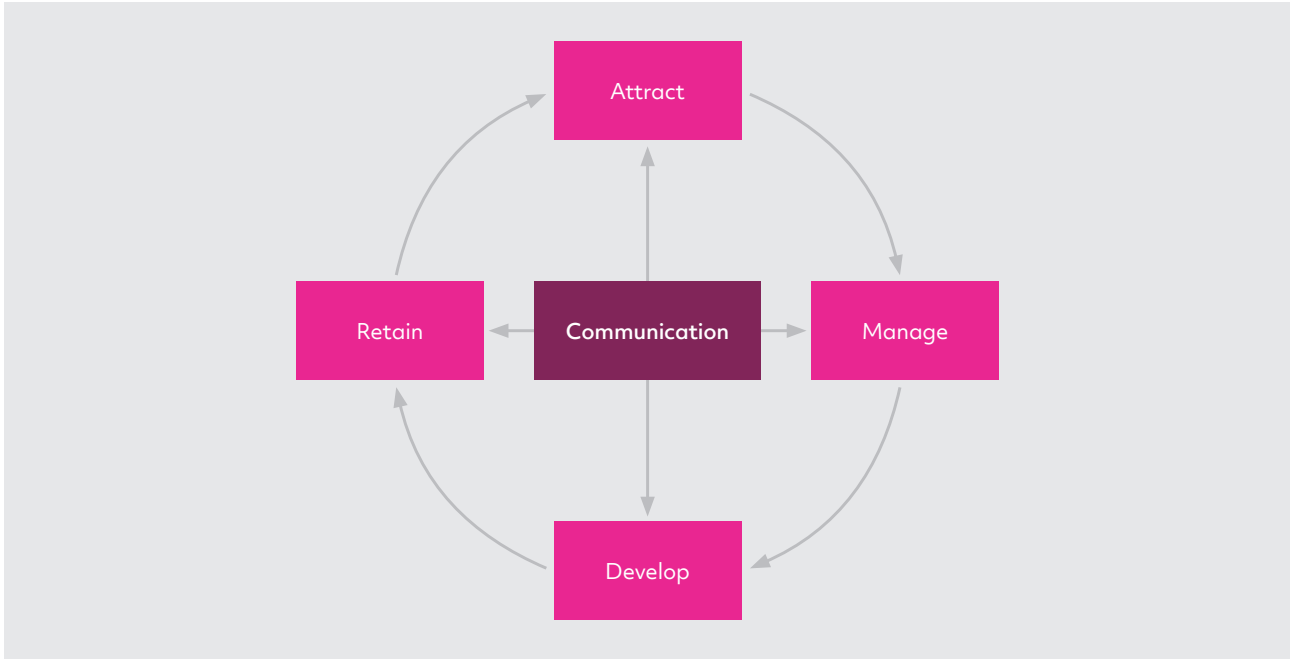
Additionally, Dalriada has developed advanced reporting tools so that detailed activity and performance information can be extracted at any point in time and, indeed, forms the basis of our standard Stewardship Reporting where administration services are provided.

AUDIT

Compliance with our procedures is subject to internal audits and external audits (AAF 01/20). The Information Security Management System ("ISMS") is subject to separate external audit for ISO/IEC 27001:2013 purposes.

OUR EMPLOYEES

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



- **Attract:** 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 ongoing 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 our client service. All our operational managers have undertaken management development training developed specifically 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; these are clearly communicated to all relevant colleagues.
- Our policies and procedures are regularly reviewed with a view to identifying and implementing continuous improvements.
- Changes to our policies and procedures are clearly communicated to all colleagues and relevant contractors.
- Compliance with our standards and relevant policies and procedures is regularly audited.

KNOWLEDGE MANAGEMENT

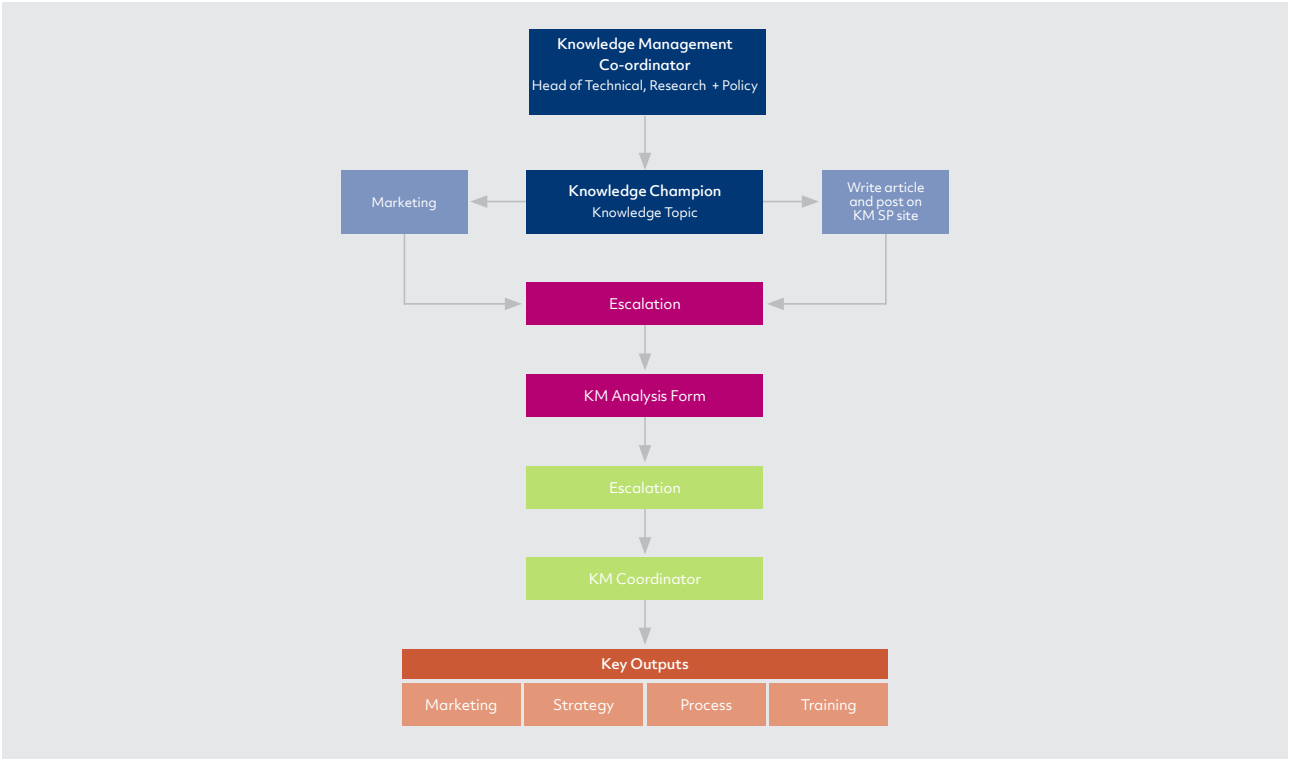
As part of our ongoing development of Knowledge Management, in December 2019, Dalriada recruited John Wilson, who has over 30 years' experience, as Head of Technical, Research and Policy'. One of the responsibilities of this role is Knowledge Management Co-ordinator.

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.
- 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 colleagues, whether or not they are Champions.
- Assessing the use and application of the knowledge and information shared on the system, and seeking to improve its presentation to ensure user friendly outputs.
- Reviewing the work of the Champions, ensuring that they are regularly updating the detail and fulfilling their KM responsibilities.
- Promoting the development of alternative approaches to communications, collaboration and information technologies that effectively support the KM processes, within and between organisations and clients, both internal and external.
- 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 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 to preserve the confidentiality, availability and integrity of that information, to ensure business continuity and to minimise business risk for us and for our clients.

Our Group has engaged a CESG Listed Adviser Scheme ("CLAS") consultant to provide information assurance advice in relation to our systems; 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 we securely dispose of information once it is no longer lawfully required.

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

Data Security

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:

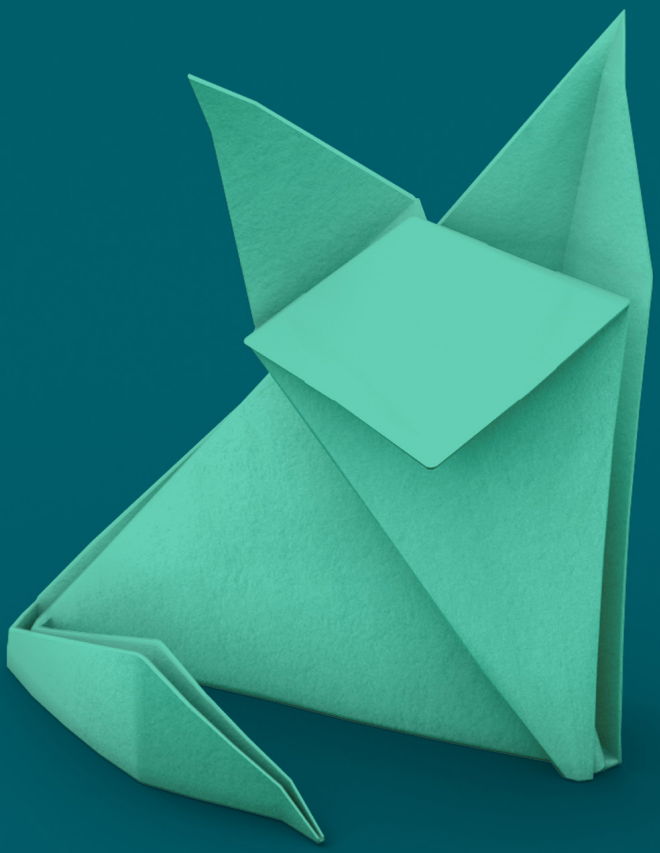
- our intended purposes for processing the personal data, and
- the lawful basis for the processing. This would apply whether we collect the personal data directly from the individual, or if it is collected from another source.

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 fellow 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, which avoids the need for storing and sharing of multiple hard copies.

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:

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 complemented 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 its core network to a highly resilient and secure MPLS offering.

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

Security

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

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

Sharepoint

We use SharePoint Online as a central resource for document management 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.

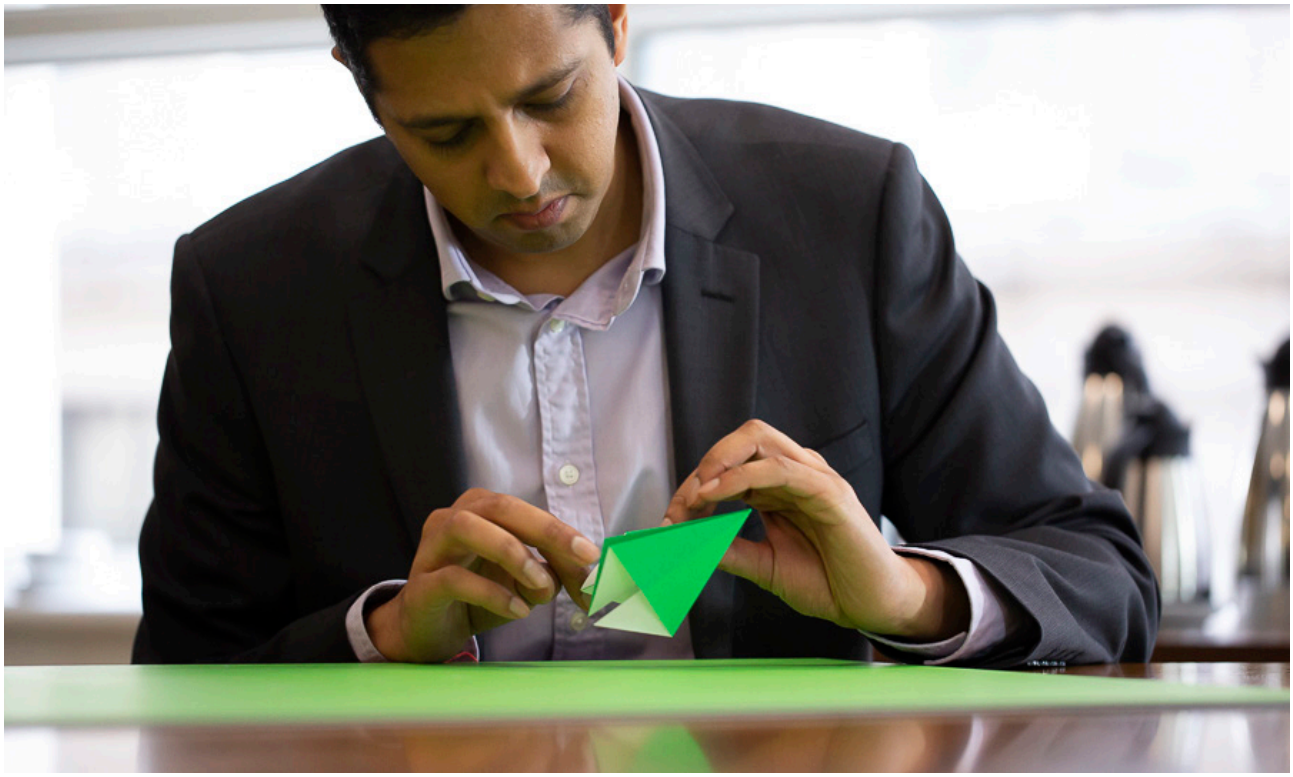
Mimecast also provides a continuity feature, whereby email can still be sent and received should an outage occur with the backend Office 365 platform.

End user computing

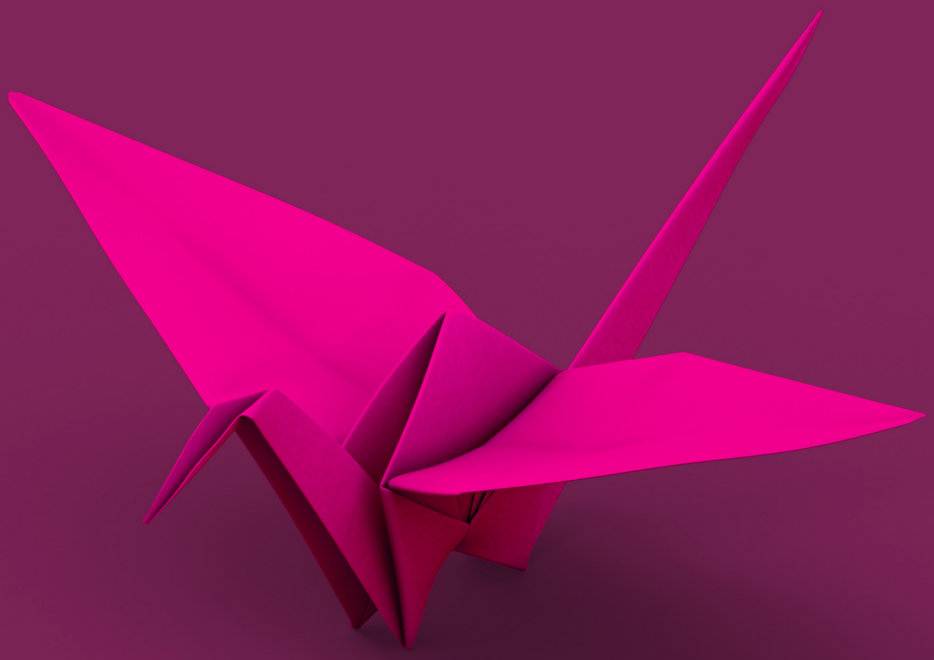
All devices are managed via industry leading Mobile Device Management ("MDM") platforms. MDM applies corporate polices to all company endpoints to ensure compliance with company security standards. Conditional based access control security measures are applied to all devices to ensure a device is compliant before it can access company data.

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 to be applied for the purpose of demonstrating 'sound administrative and accounting procedures' relating to Dalriada's own business operations for providing trustee and master trust services, and in connection with its application to remain on The Pensions Regulator's Trustee Register (under section 23(4) of the Pensions Act 1995). The design, implementation and operation of the control procedures of Dalriada provide reasonable assurance that the control objectives identified in this report are achieved.

We have evaluated the effectiveness of Dalriada's control procedures, having regard to the ICAEW Technical Release AAF 02/07, including its Relevant Trustee supplement and the criteria set out therein and the Master Trust Technical Release 05/20. The control objectives identified include all of those listed in Appendix 1 of the Relevant Trustee supplement to ICAEW AAF 02/07 and with the updated Master Trust Technical Release 05/20 produced with the assistance of a working group established by ICAEW's Audit and Assurance Faculty, which includes representation from The Pensions Regulator (the Regulator). As the control objectives are consistent with The International Standard on Assurance Engagements ("ISAE") 3000, Dalriada is reporting on both standards for this reporting period.

In carrying out those responsibilities, we have regard to the requirements of the business and the general effectiveness and efficiency of the relevant operations.

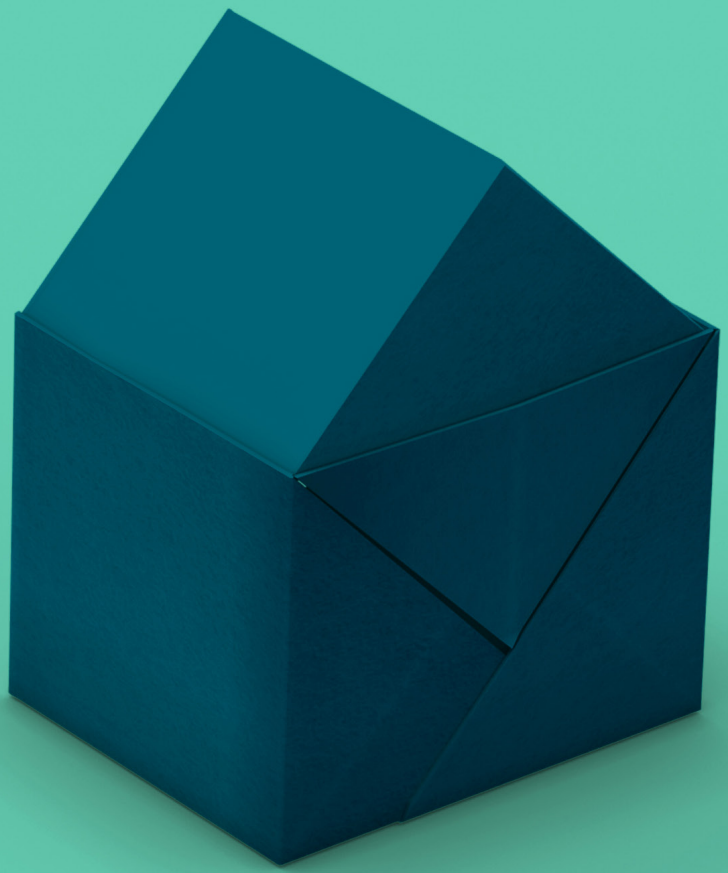
We set out in this report a description of the relevant control objectives, together with the related control procedures which were in operation during the year end 31 December 2021 and confirm that:

- the report describes fairly the control procedures that relate to the control objectives referred to above, which were in place for the period 1 January 2021 to 31 December 2021;
- the control procedures described were suitably designed throughout the period 1 January 2021 to 31 December 2021, 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 specified period.

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

Date: 25 March 2022

7 | Independent Assurance Report



7 Independent Assurance Report

RSM UK Risk Assurance Services LLP

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

Our ref: IRM/JT

Strictly Private & Confidential

REASONABLE ASSURANCE REPORT

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

23 March 2022

Dear Sirs

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 ("Dalriada or 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 21st October 2021 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 UK Risk Assurance Services LLP 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 UK Risk Assurance Services LLP will accept no responsibility or liability in respect of this report to any other party and shall not be liable for any loss, damage or expense of whatsoever nature which is caused by any person's reliance on representations in this report.

We permit the disclosure of our report, 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.

Scope

We have been engaged to report on the Organisation's description of its service organisation activities or systems throughout the period 1st January 2021 to 31st December 2021, and on the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description.

Directors' Responsibilities

The Directors' responsibility and assertions are set out on page 24 of your report. The control objectives stated in the description also include those control objectives set out in the Master Trust Supplement to AAF 02/07 that are considered relevant by trustees.

Reporting Accountant's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in that description. We conducted our engagement in accordance with the International Standard on Assurance Engagements (ISAE) 3000 and with Technical Release AAF 02/07 issued by the Institute of Chartered Accountants in England and Wales including its Master Trusts Supplement. 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 2021 to 31st December 2021.

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

Opinion

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

a) the description on pages 12 to 22 fairly presents the Organisation's controls that were designed and implemented throughout the period from 1st January 2021 to 31st December 2021;

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 2021 to 31st December 2021;

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 from 1st January 2021 to 31st December 2021.

Description of Tests of Controls

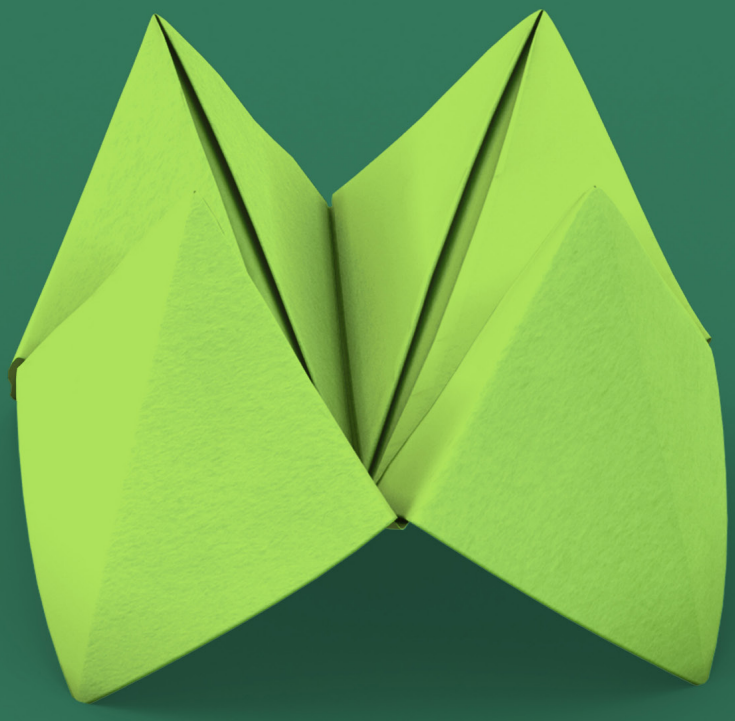
The specific controls tested and the nature, timing and results of those tests are detailed on pages 34 to 51.

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

RSM UK Risk Assurance Services LLP

RSM UK Risk Assurance Services LLP

8 | Summary of Control Objectives



8 Summary of Control Objectives

This section provides summary information and assurance on the design, description and operation of the control procedures for the administration, accounting and information technology functions for Trustee services, and governance activities for the master trust and related information technology as described in the Directors' report for Dalriada.

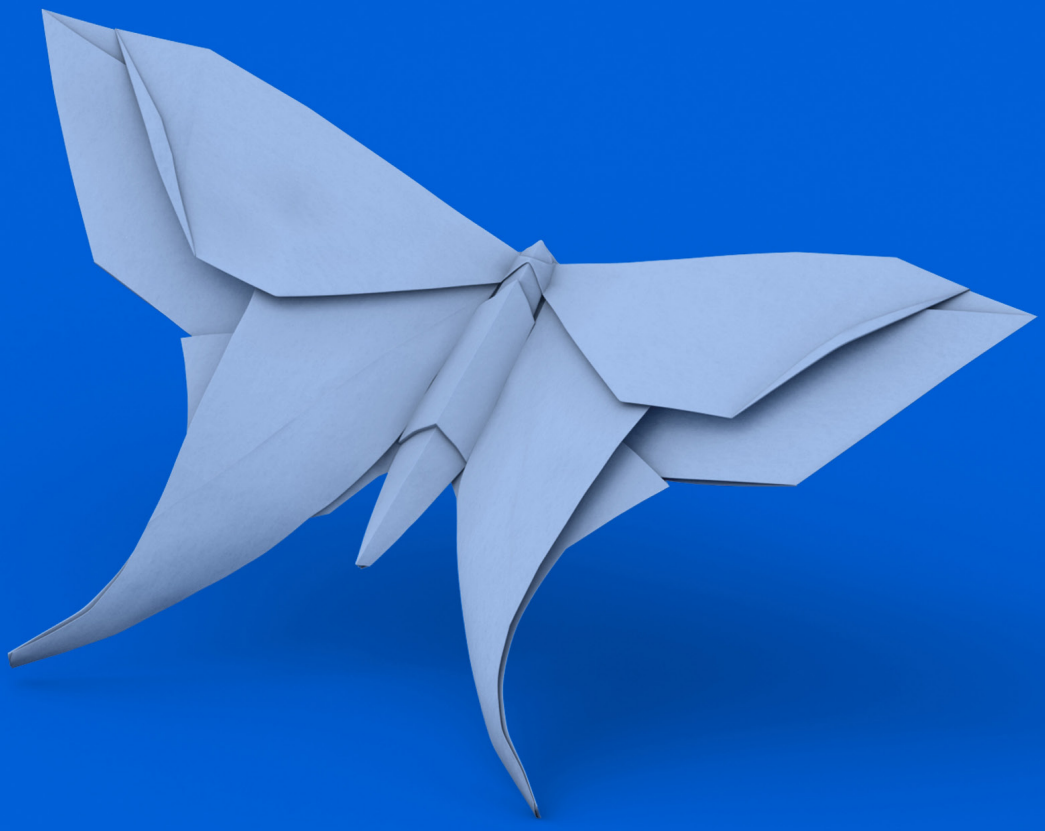
Control Objective	Audit Findings
A. Accepting Business	
A.1 Prior to accepting a new trustee appointment the risks associated with the appointment are identified, recorded, and assessed having regard to the issues facing the pension scheme, which is the subject of the appointment, given its size and complexity.	**No exceptions noted.**
A.2 Trustee appointments are accepted where the Relevant Trustee has identified and concluded that it has the sufficient level of knowledge and skill required for the trustee appointment, and has documented the steps taken in reaching that conclusion. Continuing suitability of all trustee appointments is monitored.	**No exceptions noted.**
B. Key Individuals	
B.3 Roles, responsibilities and duties of Key Individuals are documented and subject to on-going performance review.	**No exceptions noted.**
B.4 Business decisions are identified, evaluated, managed and monitored. They are recorded, properly authorised and reviewed by someone other than the decision-maker. This review is recorded.	**No exceptions noted.**
B.5 Business conflicts of interest are identified, recorded and addressed in accordance with a defined policy.	**No exceptions noted.**
B.6 The Relevant Trustee has a documented procedure for trustee appointments, which includes a documented policy for identifying, managing and monitoring actual, potential and perceived conflicts of interest for those appointments.	**No exceptions noted.**
B.7 Documented contingency plans are in place and are implemented should a Key Individual be absent.	**No exceptions noted.**
B.8 Notifications to the Regulator, including changes to Key Individuals, and periodic information returns are accurately compiled and submitted on a timely basis.	**No exceptions noted.**

Control Objective	Audit Findings
B.9 Training is conducted and training records are maintained for Key Individuals (as well as those providing services with respect to trustee appointments) in accordance with a documented training policy.	**No exceptions noted.**
C. Administrative and Accounting	
C.10 The appointment of legal advisers and other professional service providers by the Relevant Trustee is subject to a documented approach, including selection criteria and an authorisation process.	**No exceptions noted.**
C.11 The Relevant Trustee has a documented procedure for trustee appointments to monitor, on an annual basis, legal adviser's and other professional service providers' performance and compliance with contractual terms.	**No exceptions noted.**
C.12 The Relevant Trustee has a documented procedure with respect to trustee appointments for monitoring investment performance annually, having regard to the Statement of Investment Principles and investment mandates.	**No exceptions noted.**
C.13 Fees charged by legal advisers and other professional service providers to the Relevant Trustee, and fees charged by the Relevant Trustee to clients with respect to scheme appointments, are accurately calculated in accordance with the terms of appointment, suitably authorised and recorded on a timely basis.	**No exceptions noted.**
C.14 The Relevant Trustee has a documented procedure for trustee appointments to obtain scheme accounts (or other forms of summarised financial information) for the pension schemes from service providers on a regular basis in a timely manner.	**No exceptions noted.**
C.15 The Relevant Trustee's own records relating to the provision of trustee related services are accurately maintained and kept up to date.	**No exceptions noted.**
C.16 Cash and other assets held by, or on behalf of, the Relevant Trustee in respect of trustee appointments are segregated and safeguarded. Payments and receipts are suitably authorised, controlled, and recorded on a timely basis.	**No exceptions noted.**

Control Objective	Audit Findings
C.17 Minutes or other written records are maintained for all key business meetings and decisions taken by the Relevant Trustee.	**No exceptions noted.**
D Risk Management	
D.18 A review of risks which do, or could, impact on the Relevant Trustee's own business operations and trustee appointments is undertaken periodically (and at least annually). Risks are identified and evaluated, and recorded in a risk register, together with internal, controls and mitigations identified by the Relevant Trustee.	**No exceptions noted.**
D.19 Delegations (including roles and responsibilities) within the Relevant Trustee's own business are clearly documented, authorised, and monitored.	**No exceptions noted.**
D.20 Financial and compliance errors in the business are corrected promptly and a formal record and memorandum of the event is retained.	**No exceptions noted.**
E. Information Technology	
E.21 Computerised information systems have restricted physical and logical access, including appropriate measures to counter the threat from malicious electronic attack (e.g. firewalls, anti-virus etc.).	**No exceptions noted.**
E.22 Maintenance and development of systems, applications and software is authorised, tested, approved and implemented.	**No exceptions noted.**
E.23 Data and systems are backed up regularly and business and information recovery plans are documented, approved and maintained.	**No exceptions noted.**
F. Master Trust	
F24 Assessing the value for members, ensuring that annual reviews are conducted, documented, approved and maintained.	**No exceptions noted.**

Control Objective	Audit Findings
F25 Monitoring the Statement Of Investment Principles for loss, misappropriation, unauthorised use, design, ongoing suitability and default arrangement.	**No exceptions noted.**
F26 In accordance with the Master Trust Authorisation Regulations 2018, a Continuity Strategy is maintained which addresses how member entitlements and assets are safeguarded in the event of a trigger event.	**No exceptions noted.**
F.27 On appointment to a master trust, compliance with the Regulator's authorisation criteria is checked and monitored.	**No exceptions noted.**

9 | Control Procedures and Audit Testing



9 Control Procedures and Audit Testing

This section provides summary information and assurance on the design, description and operation of the control procedures for the administration, accounting and information technology functions for Trustee services, and governance activities for the master trust and related information technology as described in the Directors' report for Dalriada.

Control Objective	Audit Findings
A. Accepting Business	
A.1 As part of the client take-on process, prior to accepting a new trustee appointment any risks to the business must be identified by completing the Dalriada Accepting Trusteeship Risk Procedures Document and filed in SharePoint using the correct naming convention. Any potential risks to the business must be assessed and recorded in the Dalriada Risk Register, and discussed at the quarterly Information Security Focus Group ("ISFG") meetings, or sooner. In some instances, these may be referred to the ISFG Management Committee for further discussion and any appropriate action is taken with immediate effect. (Client Take On process 35).	Confirmed that for a sample of new schemes that the Accepting Trusteeship Risk Procedures Document was completed. Confirmed through review of Governance, Risk and Compliance meeting minutes that any potential risks identified are recorded in the risk register and discussed at the quarterly GRC meetings. **No exceptions noted.**
A.2 In being able to demonstrate that trustee representatives have sufficient capability and knowledge, they must complete the TPR online Trustee Toolkit. The online TPR Trustee Toolkit, training records and CPD records are also held and maintained by Dalriada's Human Resources Department.	For a sample of staff members, verified that the TPR Trustee Toolkit had been completed and that a record of completion of the toolkit is held on employee personnel files within the HR Talent system. Confirmed for the sampled staff that up-to-date training and CPD records are also held within their personnel files in the HR Talent system. **No exceptions noted.**
B. Key Individuals	
B.3 The Key Individuals process note explains the roles, responsibilities and duties of Key Individuals within the business and their on-going performance that is subject to periodic quality review **(Process 37 Key Individuals).** All permanent members of staff are subject to continual appraisal process. This process is continual throughout the year and closes with the output of the salary moderation meeting held in January. The appraisal completion and progress is tracked and administered by the HR Team. Key company objectives are agreed by the Board.	Reviewed the Key Individuals Process (Version 8, dated 18/10/2019) and confirmed that the roles and responsibilities for Key Individuals are clearly outlined. For a sample of Key Individuals, verified that they have been included in, and had completed, the performance appraisal process, which is tracked by HR via the Talent HR system. Confirmed the sampled Key Individuals had completed their training needs, objectives and completed system 'check-ins' as required.

Control Objective	Audit Findings
All staff meet with their line manager and agree SMART objectives aligned to the company for the next assessment period and any training or development areas are identified and flagged to the HR team. **(Process 37 Key Individuals)** To review performance against objectives set, all members of staff will meet with their relevant line manager for an informal mid-year review. Any required adjustments on the objectives set or additional training will be agreed. (Process 37 Key Individuals)	Confirmed for a sample of permanent staff, that they have been subject to an annual appraisal and an informal mid-year review which has been recorded in the Talent HR system. Confirmed for the same sample of staff, that they had completed their training needs, objectives and system 'check-ins' in the system as required. **No exceptions noted.**
B.4 To evidence that scheme business decisions are identified, evaluated, managed and monitored, Dalriada retains records of trustee meetings and minutes which are shared with client teams to ensure that all client team members are aware of actions and decisions being taken. Templates of trustee meeting minutes and agendas are held in a central location in the SharePoint governance site for retrieval. In addition, any Dalriada business decisions are discussed and agreed at the Dalriada quarterly board meetings, which are minuted and held on SharePoint. **(Client Management process 34)**	Verified for a sample of scheme trustee minutes during 2021, key actions and business decisions were discussed, were shared with the client teams and are securely stored on SharePoint. Reviewed Dalriada Q2 and Q3 2021 Board meeting minutes and confirmed evidence that key business decisions were discussed. Key Business decisions are an agenda item and discussed at each meeting. Confirmed that they are held on SharePoint. **No exceptions noted.**
B.5 All new starts are subject to an induction process, and are requested to read and sign the staff reporting requirements document to confirm an understanding of the requirements. This extends to any conflicts of interest which staff are required to disclose when commencing employment. All staff receive a conflicts of interest email so that they can flag any potential conflicts. The individual functions are responsible for reviewing the current client list with their new starts (Trustee Representative) to identify any risks. **(Recruitment Process 7)**.	Verified for a sample of new starts, any potential or perceived conflicts of interest were declared and appropriately recorded within the conflicts of interest register. We reviewed the register and confirmed that all employees, including those with no conflicts are recorded in the register. Verified, for a sample of new clients, that emails are sent to staff prior to commencement of the client work, requesting the declaration of any perceived or potential conflicts of interests so that they may be added to the conflicts of interest register. Confirmed, that where new conflicts are to arise against existing clients, it is the responsibility of the employee to bring this to the attention of the trustees as per their contract of employment. **No exceptions noted.**

Control Objective	Audit Findings
B.6 On confirmation that Dalriada has been appointed by Deed of Appointment, by the Pension Protection Fund ("PPF"), or by Order of The Pensions Regulator ("TPR") to provide trustee services, as part of the client take-on process the pre-appointment conflicts of interest documented process must be fully adhered to so as to identify, manage and monitor actual, potential and perceived conflicts of interests. If applicable, these are then subsequently recorded in the Dalriada conflicts of interest register for consideration and discussion at the Dalriada quarterly Board meetings. **(Conflict of Interest Process 33)**.	Obtained and reviewed the guidance document, Process 33, Conflicts of Interest (Version 14, 18/11/2021) to assess there was a documented procedure for trustee appointments, which includes a documented policy for identifying, managing and monitoring actual, potential and perceived conflicts of interest for those appointments. For a sample of new appointments made by the PPF and/or TPR in 2021, confirmed that a pre-appointment conflict consideration had been completed. Verified, for a sample of new appointments, emails were sent to staff prior to commencement of the client work, requesting the declaration of any perceived or potential conflicts of interests. Reviewed the conflicts of interest register and confirmed that any declarations of conflicts and declarations of nil-conflicts are recorded for each scheme. Verified that the conflicts of interest register is a standing item on the agenda of the Risk and Audit Committee, and when appropriate, the committee presents declared conflicts to the Board as part of the Risk and Audit Report. **No exceptions noted.**
B.7 Dalriada has alternate Directors in place for all clients and there is also a team of trustee representatives in place for each client. Client emails are copied in to the relevant client team members and all emails/correspondence saved onto the client SharePoint site. In the event that a Key Individual is absent for any period of time, the alternate director will take responsibility for that client and the team will direct all queries to the alternate director. The Dalriada Board will consider at what stage they need to make clients aware of an on-going absence, will ensure that clients are contacted and are aware of alternate contacts and their details. Similarly, invoicing will either be handled by the alternate director or a member of the team for the relevant clients. **(Process 37 Key Individuals)**	Verified for a sample of schemes, that there are alternate directors and staff identified for all clients and the management of conflicts has been considered. Confirmed through review of the CRM system that the five sampled clients have a listed team of consultants who complete work on their behalf. The consultants are listed in order of seniority and in any absence, the next consultant in seniority listed is responsible for client work. **No exceptions noted.**

Control Objective	Audit Findings
B.8 When a member of staff is identified as a Key Individual, the employee is asked to complete The Pensions Regulator's Trustee Toolkit. Upon completion, the employee forwards their certificate of completion to the company secretary who ensures it is filed in the employee's personnel file on SharePoint. The company secretary then forwards the relevant COR forms to the employee for completion. Once the employee has completed same, they are returned to the company secretary who forwards them to a Dalriada director for consideration and approval. Upon authorisation, the Company Secretary will then forward the completed forms to TPR by email. These forms are then ratified at the next quarterly Dalriada Board meeting. TPR will confirm that the employee has been added to the Dalriada register and again this email will be uploaded to the individual's personnel file in SharePoint. The company secretary ensures that data held by TPR is kept up to date by providing regular updates. For example, if an individual leaves ,or their details change (i.e. marriage or change of address/location), the company secretary will inform TPR by email and they will acknowledge receipt. Both emails will be filed on the individual's personnel file on SharePoint. **(Process 37 Key Individuals)**	Verified for a sample of staff members that the TPR Trustee Toolkit had been completed and the certificate of completion had been forwarded to the company secretary. Verified that the certificate of completion is held on employee personnel files within the HR Talent system. Confirmed, for the sample, that COR forms were completed by the employee and were subsequently approved by a Dalriada director prior to submission to TPR. Verified that the COR forms were ratified by the Dalriada Board at the meeting on 23 February 2021. Confirmed through review that a key individual register is maintained listing key individuals and officers and the current status of completion of their COR forms. **No exceptions noted.**
B.9 Dalriada emphasises the importance of the role that on-going training, professional qualifications and continuous personal development can play in shaping careers. All staff will have their learning and development needs reviewed bi-annually. The primary occasion for review will be at the annual appraisal. Training is monitored and approved by the training and development manager and will be provided either internally or externally via coaching, attendance at courses, seminars or professional study. Training records will be maintained, and employees who are accredited with a professional Body, and have a requirement to submit CPD hours on an annual basis, will have their CPD records reviewed on a quarterly basis to ensure that they are meeting the requirements for their professional accreditation for the year. **(Process 37 Key Individuals and Process 3 Development)**	Confirmed for a sample of staff and key individuals that their learning and development needs have been considered during their annual appraisal and mid-year review. Confirmed for the sample of employees that their training records are maintained in their personnel file within the Talent HR system. Verified for the same sample of key individuals that training records are maintained and that where applicable, CPD hours are submitted annually and reviewed on a quarterly basis. **No exceptions noted.**

Control Objective	Audit Findings
C. Administrative and Accounting	
C.10 The appointment and on-going review of third party, professional service providers by Dalriada is subject to a documented selection and procurement process. In meeting with Dalriada's minimum standard requirement, any decisions taken are agreed and minuted by the Dalriada board.	Verified for a sample of third party, professional service providers that they were subjected to a selection process and their appointment was ratified by the Board. Verified that a supplier database is in place and that it is held in SharePoint. We confirmed that supplier questionnaires are sent to all suppliers upon appointment, and annually thereafter, via an online survey platform, for completion, asking them to attach supporting evidence for answers. **No exceptions noted.**
C.11 As part of the scheme governance procedures, a review of third-party service providers is carried out at least annually and is documented in the Dalriada scheme business plan and trustee meeting agendas. Action on this is subsequently documented in the trustee meetings minutes. These are held on SharePoint, along with scheme business plans and agendas, which are held in a central location on SharePoint governance site for retrieval.	Confirmed through review of a sample of trustee committee minutes and scheme business plans, for a sample of schemes, that a review of third-party service providers is completed on an annual basis. Confirmed that trustee meeting minutes and scheme business plans and agendas are retained centrally on the SharePoint governance site for retrieval. **No exceptions noted.**
C.12 The trustee meetings agendas and scheme business plan also include a section on investment, with subsections on investment performance and strategy and an annual review of investments. Documented action on this, following on from the meetings is recorded in the trustee meeting minutes.	Confirmed for a sample of schemes that a section on investment performance is included in the scheme business plans. Confirmed through review of trustee meeting agendas and minutes for the same sample of schemes, a section on investment performance and strategy was included and the investment performance monitoring report was included. **No exceptions noted.**
C.13 Dalriada's contractual agreements are by way of Deed of Appointment and/or Letter of Engagement with the Company. These are scanned onto SharePoint and filed in the SharePoint client folder.	Verified for a sample of new schemes that an appropriate Deed of Appointment document or Services order form is in place, and that it has been signed by the trustees of the scheme and Dalriada client management.

Control Objective	Audit Findings
Hard copies are held securely off-site. Billable time is recorded and the client invoicing schedules are distributed to the appropriate trustee representative. Upon review and approval for invoice, the Corporate Finance Function is instructed to create and issue the invoice. Invoices received by Dalriada from third parties are reviewed for completeness and accuracy, authorised and passed to the relevant party for settlement. If this is to be settled by Dalriada it will be sent to the pension fund accounting team together with approval to settle, otherwise the invoice is sent to the appropriate third party together with the backing schedules, which provide extensive details of the tasks carried out.	Confirmed via a walkthrough of the billing process that trustee representatives record time through the Add Time function to the relevant project or scheme. For a sample of invoices, we confirmed that the Corporate Finance Function reviewed the Invoice Ready system and prepared the invoice and other supporting documentation to be sent to the client. Verified for the same sample of invoices, that an email was sent to the client with the standard invoice, time cost detail and fixed fee as per the client invoicing schedule. Verified for a sample of invoices received that appropriate review and authorisation is completed prior to payment being made. Verified that the sampled invoices are authorised and an email is retained on the system from the authoriser and attached to the payment information. **No exceptions noted.**
C.14 Dalriada's pension fund accounting team is notified as one of the intended recipients on the initial take-on document, which forms part of the client take-on process regarding the production of scheme accounts. The pension fund accounting team records whether the scheme accounts are prepared internally, or are carried out externally. A register documenting each set of accounts prepared either internally, or externally, is circulated to all trustee representatives summarising the progress to date. **(Pension Fund Accounting Process 27).**	Confirmed that Dalriada's pension fund accounting team and the Fund Accountant is documented as one of the intended recipients on a sample of clients' take-on documentation. Verified that a register outlining if scheme accounts are prepared internally and externally is in place, and are located within the CRM system. **No exceptions noted.**
C.15 Dalriada maintains financial management controls to ensure proper records are maintained and kept up to date. All employees record their time in our in-house bespoke workflow system. Time is recorded against client codes. At the beginning of each month a billing cycle is created and a schedule detailing all time recorded to the client code during the period is sent to the appropriate trustee director, or trustee representatives, for review via the invoicing application. Once the trustee director or trustee representative has reviewed the content, they will approve the time on the invoicing application and use the invoicing application to submit the invoice to finance for issue.	Verified for a sample of invoices that invoice amounts are calculated using the timesheet information entered into the workflow system by Dalriada employees. Verified, for the sample of invoices, that a schedule of all recorded time against the client code for the billing period is sent to the client manager for review and subsequent approval in the Review Invoice system. Confirmed that once, approved, the invoices are submitted to corporate finance for preparation and issue.

Control Objective	Audit Findings
The corporate finance team reviews the invoice approval, submits the invoice to our accounting software and issues the invoice to the client, by post or by email, along with the appropriate backing documentation. Statements are issued to clients on a monthly basis and any outstanding debt is actively followed up. The corporate finance team has access to online banking and has weekly calls to discuss outstanding debt. Monthly management accounts are produced and circulated to senior management within the group and monitored against budget. Revenue and productivity figures are monitored on a weekly basis and the information circulated to relevant senior management. **(Corporate Finance – Bank and Cash Process 23)** Belongs to the above C15 section - On appointment, Dalriada issues each client with details of the basis on which it will be invoiced, including charge out rates and, where appropriate, budgets for the expected work. Invoices are compared with the agreed basis to ensure budgets are not breached. If applicable, a fixed fee schedule is maintained which sets out the amount of the fee, the frequency of billing and any agreed increases as set out in the terms of appointment. This enables accurate and timely billing.	For the sampled invoices, confirmed that the Corporate Finance Function accessed the Invoice Ready system and prepared the invoice and other supporting documentation to be sent to the client on a monthly basis. Verified for the sampled invoices, an email was sent to the client with the standard invoice, time cost detail and fixed fee as per the client invoicing schedule. Confirmed that the corporate finance team has access to online banking, and confirmed that weekly calls are scheduled every Friday to discuss outstanding debt. **No exceptions noted.** Confirmed for a sample of schemes that Dalriada issues each client with details of the basis on which it will be invoiced, including charge out rates and, where appropriate, budgets for the expected work. Confirmed, for the same schemes, that the Corporate Finance Function monitor budgets vs expected client work. Further confirmed for the five schemes that the Corporate Finance Function sends a quarterly report to client managers outlining time recorded vs budget, expected revenue and recoverability percentage. **No exceptions noted.**
C.16 Dalriada uses an off-the-shelf accounting software package to maintain its financial records. Each scheme has its own bank account and the financial records are maintained separately. The client and corporate accounts sit on separate network folders only accessible by authorised staff. Passwords are required to access each scheme account, which are kept separate from the corporate accounts. **(Pension Fund Accounting Process 27).**	Confirmed through review that Xero and QuickBooks accounting software is used to maintain financial records. Confirmed for a sample of schemes that each scheme has its own bank account. We further confirmed through a system review that bank accounts and financial records for each scheme are held separately within the system. Confirmed that access to scheme records and accounts is only granted by staff entering their unique username and password to log into the system. Confirmed that staff can only access the schemes in the network, and on Mantle, of which they are an authorised team member. **No exceptions noted.**

Control Objective	Audit Findings
C.17 To evidence that business decisions are identified, evaluated, managed and monitored at the Dalriada quarterly Board meetings, Dalriada retains minuted records of the meetings, Board resolutions and authorised signatory listings. These are drafted by the company secretary, agreed and signed by the Board, and maintained and held in the governance site in SharePoint for reference purposes. **(Client Management Process 34)**	Reviewed Dalriada Q2 and Q3 2021 Board meeting minutes on SharePoint and confirmed evidence that key business decisions were discussed. Reviewed the most recent Board Resolution document dated 30 June 2020 detailing the reviewed and updated authorised signatory listing. **No exceptions noted.**
D. Risk Management	
D.18 Dalriada's risk management process involves the identification of a variety of risk scenarios on a risk register, and the recording of the associated threats and vulnerabilities that might be exploited by the threats. Existing controls in place are noted and an overall risk rating is calculated. This methodology ensures that on-going risk assessments produce comparable and reproducible results. If applicable, a Risk Treatment Plan is formulated, escalated and formally approved. This provides the basis for knowingly and objectively accepting/treating risks or deferring the possibility of implementing the countermeasures into the planned future. The risk register is reviewed at planned intervals with the GRC, taking into account changes to the organisation, technology, objectives, identified threats, legal, regulatory and contractual requirements. Risk scenarios are drawn up in the quarterly GRC meetings via a cross section of staff from the different areas of the business. All members of staff are required to report any potential risk scenarios to the GRC (**Risk Management Process 19)**. The GRC report to the Dalriada board quarterly and appropriate action is agreed.	Verified that a risk register (version 133, dated 14/12/2021) is in place which is subject to review on a quarterly basis. Verified that a Risk Treatment Plan has been formulated for each risk and the plans are detailed alongside the risk in the risk register. Confirmed for Q2 and Q3 Board meeting minutes and verified a risk register update was presented to the Board as part of the Risk and Audit report. Verified for a sample of risks, which included a risk relating to a data migration project, that existing controls are documented, risk ratings and scenarios are assigned and a planned review of the risks is documented to be completed at the next GRC meeting (15/02/2022). Confirmed through review of Q2 and Q3 2021 GRC meeting minutes that an update on the risk register was provided and review of the risks outlined on the risk register was completed by the meeting attendees. **No exceptions noted.**
D.19 Board resolutions for Dalriada and authorised signatory listings are held in the governance site in SharePoint for reference purposes. This provides clear guidance on the signatories and authorisations for bank accounts, investment instructions and authorised signatories.	Reviewed the most recent Board Resolution document dated 30 June 2020, detailing the reviewed and updated authorised signatory listing. Confirmed that the Board is in the process of updating the Resolutions as part of an internal project to make the process of resolution signing a digital one.

Control Objective	Audit Findings
	Confirmed, through review of SharePoint, that the resolutions are held in the governance site for reference purposes. Confirmed that it contained guidance on the signatories and authorisations for bank accounts, investment instructions and authorised signatories. **No exceptions noted.**
D.20 Procedures are in place for errors & omissions and compliance breaches, whereby any transaction errors are notified immediately by the scheme administrator to their line manager and the trustee representative. Details are recorded in the Incident Management Application and held on SharePoint. This is also reported to the GRC and must be followed up to the point of conclusion. All errors & omissions and regulatory breaches are notified to the Board of Directors as part of the internal management information reporting process. The trustee representative will determine if any further action is required and will notify the relevant parties to implement. The trustee representative should then determine if a regulatory report is required to be completed and submitted to TPR.	Verified that there is an Incident Management process document in place (version 15, dated 17/01/2022) which deals with the procedures to follow in the cases of errors, omissions and compliance breaches. Confirmed that the Incident Management Application has been implemented for the recording of all incidents, omissions, regulatory and DPA breaches. Verified through review of a sample of errors, omissions, regulatory breaches, DPA breaches and complaints, that they were appropriately recorded, with incident date, incident number, responsible party, incident details, locality, departmental area and resolution outlined. Confirmed through review of minutes for the GRC in 2021, that incident reporting is a standing agenda item and the status of all incidents recorded are discussed. Reviewed the Dalriada Q2 and Q3 2021 Board minutes, and confirmed that errors, omissions and breaches are reported to the Board as part of the Risk and Audit Report. Confirmed that presentation of the Report is a standing item on the agenda for quarterly Board meetings. Reviewed a sample of regulatory breaches and confirmed that, when necessary, regulatory reports were completed and submitted to the TRP. **No exceptions noted.**

Control Objective	Audit Findings
E. Information Technology	
E.21 The primary IT infrastructure resides at a secure, ISO 27001 certified, world class, off-site data centre utilising Infrastructure as a Service (IaaS) Dalriada's full environment is replicated to a second Azure region (UK West). Windows laptops are configured by an automated build to have password protection and data encryption is enforced. Corporate Anti-Virus and Device Configuration policies for Windows, MacOS and Mobiles are managed via InTune This enforces the same Security Baseline across the company.	Observed the Microsoft Azure Recovery Services and confirmed 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). Observed the Microsoft Azure Recovery Services and confirmed that the replication status was noted to be healthy and protected, with the last failover test performed in January 2022, with no configuration issues noted. Inspected the configuration on InTune (Microsoft Endpoint Manager) and confirmed that all devices are onboarded on InTune and have password protection and encryption settings aligned to the compliance policy for the operating system of each device. Observed that all devices Anti-Virus and Device Configuration policies and confirmed that they are managed through InTune for all the operating systems. **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 15 characters in length, alpha numeric. This is detailed in the company's Security and Confidentiality Policy for staff and is backed up by the Access Control Process.	Confirmed through review of the InTune platform that each operating system has a compliance policy that requires all access to computer equipment and systems to be protected by passwords. Inspected the password setting on the domain and noted that passwords are set to expire after 42 days, password complexity is enabled, with a minimum password length of 14 characters. Inspected the Security and Confidentiality Policy and noted that the password requirements set out in this policy are aligned to the configuration set in the domain security policy noted above. **No exceptions noted.**

Control Objective	Audit Findings
All data is stored on the corporate network and data is only permitted to be stored locally on laptops that are corporate owned, and registered within MDM solution. Access to data stored on the network is restricted using appropriate permissions. Functional groups of users are maintained, each with appropriate levels of access permissions. Only Internal IT can amend an individual's permissions outside of SharePoint Team access. Otherwise team owners can authorise access to SharePoint sites. Access rights are reviewed and amended as necessary i.e. when roles change or new members of staff join the company. Details of the restrictions in place on the network are documented.	Inspected the Microsoft Endpoint Manager admin centre and confirmed that all corporate devices are registered and managed on InTune. Observed access settings and confirmed that only IT administrators can change access permissions. Inspected the Azure AD Authentication methods and confirmed that multi-factor authentication is used to access data remotely. Observed user access setup and confirmed that users are assigned access through functional groups and these groups are maintained with appropriate levels of access permissions. Inspected a sample of new users and confirmed that user access required line manager authorisation prior to user access being actioned by IT. Inspected a sample of access reviews and confirmed that colleague profiles are reviewed on a quarterly basis by the colleague's manager and are amended by IT when a colleague changes roles or leaves the company. We were not able to inspect any evidence of a user with a role change for the period under review. **No exceptions noted.**
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, pensions administration etc. are restricted to only those who have the associated privilege. User access is approved by line managers and actioned by Internal IT. Access to the administration systems is controlled by windows authentication two factor authentication and utilising Privileged Identity Management. Where possible, this requires users to enable Administrative Roles when required. Segregation of duties and rules are enforced by security profiles built into the administration system. Profiles are assigned to authorised individuals and aligned to their roles and responsibilities.	Inspected a sample of new users and confirmed that user access required line manager authorisation prior to user access being actioned by IT. Inspected the functional groups that are used to assigned user with access relating to their job function, and noted that access is restricted to those users assigned to each group. Through inspection of the IT Members group, confirmed that the users in this group are limited to the internal IT team. Inspected the Azure AD Authentication methods and confirmed through observation that multi-factor authentication is enforced on all users, including those who have access to administration systems.

Control Objective	Audit Findings
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.	Observed user access setup and confirmed that users are assigned access through functional groups and these groups are maintained with appropriate levels of access permissions, ensuring segregation of duties and rules are enforced as each group is set up in a way that gives user access only to that which is required in line with their roles and responsibilities. Verified that different levels of security profiles are built into the administration system, restricting unauthorised access. **No exceptions noted.** Inspected the IT system and confirmed that all users are allocated a unique network user ID and password and access privileges are set according to job roles. Through inspection of scheme setup, confirmed that each administrator has limited access only to the records and data of only the schemes they have been given access to. **No exceptions noted.** Inspected the audit trail facilities in place and confirmed that an audit trail of changes made to data, including who made the changes and when, is kept. **No exceptions noted.**
All IT processing is carried out on laptops in real time. Email and MS Teams are used as the electronic means of communication in the business. Dalriada utilises SharePoint and Azure AD guest accounts for controlling access to SharePoint Online. Conditional access controls are in place for all guest accounts, to force the use of Multi Factor Authentication. The business utilises a combination of Microsoft Outlook and Microsoft Exchange Server to handle the storage and delivery of all business email. Individual staff members are responsible for complying with the Security and Confidentiality policy for password protecting documents containing confidential, personal and sensitive data.	Observed a visual timeline of online processing activity by users and confirmed that all processing is carried out in real time. **No exceptions noted.** Observed the SharePoint secure portal and confirmed that it is used for the sharing of information externally, where user access rights are confirmed. Through observation of a sample of SharePoint and AD guest accounts, confirmed that Dalriada utilises these to control access to SharePoint Online. Observed access settings and confirmed that only IT administrators can change access permissions. Inspected the Azure AD Authentication methods and confirmed that multi-factor authentication is used to access data remotely.

Control Objective	Audit Findings
	Through observation, we confirmed that the business utilises Microsoft Outlook and Microsoft Exchange Server to handle the storage and delivery of all business email. Inspected a sample of new users and confirmed that user access required line manager authorisation prior to user access being actioned by IT. **No exceptions noted.**
All external access to the network is authorised internally by the Head of IT . Remote access is then setup by Internal IT and connections can only be made through Windows Virtual Desktop. The company contracts WaveNet to host a Firewall within its datacentre to control port access in and out of the business. All email traffic is routed by a third party, Mimecast, which filters out any email threats i.e. viruses/ spyware and inappropriate content. Inappropriate content also triggers a rules-based alerting system that keeps staff members aware of any trends requiring action. Windows Defender software is installed on all servers, desktops and laptops and is designed to keep users safe from viruses and other forms of on- line malicious threats. Anti-Virus software is installed on all servers, desktops and laptops and is designed to keep users safe from viruses and other forms of on-line malicious threats.	Inspected a sample of external network access request and confirmed that network access is required to be authorised by the Head of IT. Inspected the Windows Defender software and confirmed that it is used to provide anti-virus protection and that it is installed on all devices, and at the time of the walkthrough all devices had no active malware. Observed Microsoft Outlook email settings and confirmed that Mimecast is used to monitor email traffic and remove threats. Inspected the WaveNet agreement in place and confirmed that WaveNet is used to provide firewall protection. Inspected the Default Windows Defender Anti-Virus Policy and confirmed that scanning of all incoming and outgoing traffic, including emails. Through a sample of external emails, confirmed that Mimecast is being used to filter out any email threats. **No exceptions noted.**
E.22 Any changes to existing or the implementation of new, infrastructure and systems follows the Operational Change Control process outlined in the Operations Security Process 12). A major change will typically be a planned implementation and this will be discussed at IT Subcommittee. When a major change is required, business impact is reviewed and formal sign off and authorisation is required. **(Operations Security Process 12).**	Inspected the Operations Security Process and noted that it includes the Operational Change Process, which provides guidelines on any changes to existing or the implementation of new infrastructure and systems. Inspected an internal change log and confirmed that this is maintained within the IT Service Desk as per the change management procedures. Inspected a sample of changes carried out by Internal IT in 2021 and confirmed that approval, potential impact, roll out plan, back out plan and testing were recorded. **No exceptions noted.**

Control Objective	Audit Findings
E23. Dalriada has also adopted an effective Information System Acquisition, Development, and Maintenance Process (14). Controls are in place to ensure the installation and upgrading of operational software on each operating system. Any maintenance is performed by authorised representatives from the corresponding software/ support company and is pre-arranged. Notice is given to colleagues of any downtime to the network that is required for the maintenance of software.	Inspected the Information System Acquisition, Development, and Maintenance Process and confirmed that Dalriada has an effective process in place. Confirmed that there were no Information System acquisitions, upgrades or development on any system in the period under review. Observed software update settings and confirmed that there is an automatic control in place for application updates for Apple Macs and Windows. Inspected the HTG agreement in place and confirmed that Citrix application updates are provided by managed service provider HTG. Updates are not authorised to be completed between the hours of 8:00-18:00. Verified for a sample of notifications sent to staff informing them of system maintenance. **No exceptions noted.**
Any software upgrades are performed only if there is a requirement to do so, or suitably long enough after the release, to ensure any bugs or vulnerabilities have been ironed out. If new software potentially introduces any element of risk, then the risk will be assessed and its advantages of functionality will be subject to continued monitoring and/or isolated. Windows updates are rolled out periodically to all computers on the network.	Confirmed that there were no software upgrades on any system in the period under review. As such, we could not obtain any evidence to demonstrate how this control is operating. Inspected the configuration of the Azure Patch Management, which is managed through InTune, and confirmed that windows updates are rolled out on a regular basis to all computers on the network. **No exceptions noted.**
Development of systems is facilitated by an appropriate rollback strategy. The pensions 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 pensions database team manager to ensure procedures have been followed. 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.	Inspected a sample of change carried out by Internal IT in 2021 and confirmed approval, potential impact, roll out plan, back out plan and testing were recorded. Inspected the configuration of InTune and 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 update warnings have been issued. There were no data migration projects to test during the year. We could not inspect evidence of to ensure the procedure in place was followed. **No exceptions noted.**

Control Objective	Audit Findings
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.	Observed the Microsoft Azure Recovery Services and confirmed 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. Inspected the Microsoft Azure Recovery Services vault and confirmed that Azure Site Recovery is in place which enables automatic data recovery. Inspected the BCP Testing Schedule and results 2012 – 2022 and verified that disaster recovery testing of the IT infrastructure is completed on a 90-day cycle and is in line with BCP plan. **No exceptions noted.**
Backup and Restore Technology All servers in Azure are backed up on a daily basis from 22:00 23:30 UTC. SQL Databases are backed up in Full starting at 19:30 UTC with transaction log backups running continuously every hour on supported databases. Recovery snapshots are held for two days and daily backups are retained for 30 days, with Dalriada retaining a weekly backup for three months 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 one hour Recovery Time Objectives ("RTO") of under four hours for the entire virtual estate.	Inspected the backup schedule for servers on Azure and confirmed a daily back up process is in place and there is a retention of 30 days, maintained with the backup vaults. Inspected the backup schedule for SQL databases and confirmed that they are backed up in full, starting at 19:30 UTC, with transaction log backups running continuously every hour on supported databases. Inspected the BCP Testing Schedule and results 2012 – 2022 and confirmed failover tests of Azure (UK South) to Azure (UK West) have been conducted in 2021 with recovery times achieving a Recovery Point Objective ("RPO") of one hour. **No exceptions noted.**

Control Objective	Audit Findings
F. Master Trust Framework	
F24 A value for money assessment is undertaken annually and the process followed is documented and approved. The assessment includes value to members derived from scheme management and governance, administration, investment governance and communications. Disclosure of information to members of costs and charges (rates %) and or/amounts (£) are complete and accurate.	Confirmed through review of the Annual Report (dated 31st March 2021) for the one master trust in place that a value for money assessment was completed. Confirmed that the assessment included member charges, governance, administration, communication and investment performance. **No exceptions noted.**
F25 Scheme and member assets or entitlements are safeguarded from loss, misappropriation and unauthorised use. The financial protection and compensation available to members in the event of a default is assessed and documented. The design and ongoing suitability of the default arrangement and range and risk profile of other investment options are regularly reviewed and monitored. This review is documented and the investment aims and objectives for the arrangement, and investment policies for all investment options, are included in an appropriate Statement of Investment Principles. The performance of each investment option, including the default arrangement(s) in which member funds are regularly reviewed and monitored against objectives, is contained in the Statement of Investment Principles. This review is documented and approved. The trustee ensures the Statement of Investment Principles is publicly available.	Verified through review of a scheme's Annual Report (dated 31st March 2021) for the one master trust in place, that a written Statement of Investment Principles (SIP) is prepared and maintained by the trustees. Confirmed through review that the SIP assesses the protection available to members in the event of a trigger event and that it considers two Continuity Options that the trustee may decide between in the case of an event occurring. Confirmed by way of review of the trustee minutes that the suitability of the default arrangements and the investment strategy is reviewed on an annual basis and is included in the updated SIP, which was formally adopted by the trustee on the 26th April 2021. Confirmed by way of review that the SIP outlines the principals governing the investment policy of the trust and the activities undertaken by the trustee to ensure the effective implementation of these principles. Verified that the SIP has been made available to the public. **No exceptions noted.**

Control Objective	Audit Findings
F26 In accordance with the Master Trust Authorisation Regulations 2018, a Continuity Strategy is maintained which addresses how member entitlements and assets are safeguarded in case of a trigger event.	Verified through review of the Continuity Strategy (Version 4.0, April 2021) for the one master scheme in place, that it clearly outlines how member assets are safeguarded. Confirmed that the Continuity Strategy is subject to review on an annual basis every April Confirmed by way of review of the trustee minutes that the Strategy was approved in the Q2 meeting. **No exceptions noted.**
F.27 On appointment to a master trust, compliance with the Regulator's authorisation criteria is checked and monitored.	Verified that there is a Continuity Strategy in place which details the procedures to follow in the event of a trigger event. Verified that it details the roles and the responsibilities of those with control over the administration of the trust, considers the financial suitability and relative financial costs of continuity strategies and demonstrates that the funder of the scheme is able to financially support the trust. Confirmed that there is an annual business plan which is maintained and that risks are recorded in a risk register which is reviewed on a quarterly basis. **No exceptions noted.**

Appendices

Appendix 1- Letter of Engagement

RSM Risk Assurance Services LLP

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

Our Ref: IMc/tal

21 October 2021

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

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 02/07 issued by the Institute of Chartered Accountants of 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 THE 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 Director's 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 ('Director's 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 02/07 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 administration, accounting and information technology function, 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 02/07, issued by the Institute. Our work will include enquiries of management, together with tests of certain specific control procedures which will be set out within the AAF 02/07 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 02/07 issued by the Institute.

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

We may seek written representation 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 bought 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 of the Organisation and to the potential customers ('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.

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 the use of the disclaimer wording being used as 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 Risk Assurance Services LLP *neither* owes nor accepts any duty to Third Parties and shall not be liable for any loss, damage or expense of whatsoever nature which is caused by their reliance on our Report. Should any Third Party choose to rely on 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 the RSM Risk Assurance Services LLP against all actions, proceedings and claims brought or threatened against the RSM Risk Assurance Services LLP 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 Risk Assurance Services LLP's work under this engagement letter.

AGREEMENT OF TERMS

We shall be grateful if you could confirm in writing your agreement to these terms by signing and returning the enclosed copy of this letter or let us know if they are not in accordance with your understanding of our terms of engagement.

Yours faithfully

RSM Risk Assurance Services LLP

Encs. Terms and Conditions of Business dated May 2018

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

Signed ..... Date 05/11/2021

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

St James Tower
7 Charlotte Street
Manchester
M1 4DZ