

Columbia Threadneedle Investments EMEA

ISAE 3402 / AAF 01/20

Contents

Columbia Threadneedle Investments EMEA – Introduction and Scope of Report.....	3
Service organisations’ management statement on controls at Threadneedle Asset Management Limited and Threadneedle International Limited, together referred to as “Columbia Threadneedle Investments EMEA” (the “Service Organisations”)	6
Management’s Statement by management of Columbia Management Investment Advisers, LLC	8
Management’s Statement by the Directors of Ameriprise Financial, Inc.	10
Independent service auditor’s assurance report on controls at Threadneedle Asset Management Limited and Threadneedle International Limited (the “Service Organisations”)	12
Section I – Description of the Control Environment and Client Control Considerations	15
1. Global Governance	15
2. Regional Governance.....	15
3. Enterprise Risk Management Framework	17
4. Information Technology	20
5. Human Resource Policies and Procedures	23
6. Investment Management Approach.....	23
7. Client Management	25
8. Amendments and Exclusions	26
9. Complementary User Entity Controls.....	26
Section II – Control Objectives, Related Controls and Service Auditor Testing and Results	28
Section III – Management Responses.....	88
Section IV – Information provided by the Service Auditor.....	91
Use of Management Testing	92
Appendix I – Prospective Client Disclaimer Letter	93
Appendix II – Important information.....	95

Columbia Threadneedle Investments EMEA – Introduction and Scope of Report

Columbia Threadneedle Investments is the global asset management business of Ameriprise Financial, Inc. (NYSE: AMP), a leading US diversified financial services company and one of the 50 largest asset management firms globally¹.

Columbia Threadneedle Investments markets its products to investors through a wide range of product structures (e.g., segregated accounts, UK Life structures, UK Open Ended Investment Companies (OEICs), and Luxembourg Société d'Investissement à capital variable (SICAVs)).

The Boards of Directors of Threadneedle Asset Management Limited and Threadneedle International Limited are together responsible for the management of the institutional businesses of Columbia Threadneedle Investments EMEA (Europe, Middle East and Africa), excluding Real Estate and Infrastructure. In particular, these Boards are responsible for the design and the effective and continuing implementation and supervision of the control environment operated by Columbia Threadneedle Investments EMEA. In designing these controls, the Boards have regard to the interests of clients, the regulatory environment, and the effective and efficient operation of the institutional business.

Key facts and figures – Columbia Threadneedle Investments (as at 30 September 2023)

- AUM: £482 billion (US\$587 billion)
- Over 2,500 people globally, including more than 650 investment professionals
- Present in 19 countries across Europe, Middle East, Asia Pacific, North America.

Overview and Scope of Report

This report covers the investment management and all UK managed and serviced client reporting activities for institutional clients contracted to Threadneedle Asset Management Limited and Threadneedle International Limited (the "Service Organisations"), collectively the asset management companies of Columbia Threadneedle Investments EMEA, with the exception of Real Estate mandates which are covered by the Columbia Threadneedle Investments Real Estate ISAE 3402/AAF 01/20 report and controls relating to Columbia Threadneedle AM (Holdings) plc, its subsidiaries

and Columbia Threadneedle (EM) Investments Limited which are covered by a separate ISAE report. This report is designed to provide information about Columbia Threadneedle Investments EMEA's controls to client organisations and their independent auditors.

Inclusive Subservice Organisations

This report is produced using the 'inclusive method' for Columbia Management Investment Advisers, LLC (CMIA) and Ameriprise Financial, Inc. (AMPF) which operated middle office and information technology controls. This means that the controls carried out by the subservice organisations have been subject to testing by PricewaterhouseCoopers LLP (PwC) as part of their reporting.

Carved-Out Subservice Organisations

The report is presented using the "Carve-Out" method for processes and controls carried out by Columbia Threadneedle Investments EMEA's third party service providers and these controls have not been subject to independent testing by PwC as part of this review. The only exceptions to the "Carve-Out" method are controls which specifically relate to EMEA funds and are operated by CMIA and AMPF. Those controls are included in this report and are independently tested by PwC.

The report describes the controls related to the acceptance of clients, authorisation and processing of transactions, maintenance of financial and other records, compliance monitoring, and reporting to clients, together with the supporting information technology controls. All control procedures in operation throughout the period are clearly outlined in Section II of the report.

The scope of this report does not cover controls relating to the fund management decision making process. Neither does it cover controls relating to business undertaken in Asia or North America.

The subservice organisations carved out of this report include:

- HSBC Securities Services (HSS) – undertakes fund accounting services for certain clients of Columbia Threadneedle Investments EMEA;
- Citi – undertakes Fund Accounting; Custody and Depositary services for the UK and Luxembourg regulated funds;

¹ Source: IPE Top 500 Asset Managers 2023 rankings, September 2023.

- BlackRock Solutions (BRS) – Hosts the BlackRock Aladdin application that provides portfolio and trade management, risk management, security master data and corporate action event management and processing for Equity, Fixed Income and Multi-Asset Allocation Portfolios;
- Fidelity National Information Services (FIS) – Hosts the InvestOne application that facilitates the collection of security prices;
- Global Switch - IT data centre host, managing all associated physical security related controls and all environmental aspects (i.e., power, climate, etc);
- Kyndryl – Provides certain computer operations and infrastructure support services for the in-scope application at the St. Louis (US) Data Center;
- Factset – Portware is hosted at Factset and provides multi-asset execution management system for the creation and execution of algorithmic trading strategies for global equities, futures, options, and FX.

It should be noted that neither Threadneedle Asset Management Limited nor Threadneedle International Limited are authorised to hold client money. It should also be noted that client money and custody assets are held in an account opened by the client and controlled by their custodian. Columbia Threadneedle Investments EMEA is not responsible for the appointment of third-party service providers in respect of safe custody of client's assets. Whilst related controls (e.g., those pertaining to the selection and oversight of custodians) are excluded from this report, custodians' positions are regularly validated against Columbia Threadneedle Investments EMEA's positions through the daily reconciliation processes.

The report contains the following:

- A Service Organisation's Statement prepared by management providing an assertion on whether controls related to the control objectives stated in this report were suitably designed and operated effectively throughout the period 1 October 2022 to 30 September 2023, and that the descriptions in Sections I and II of this report fairly present Columbia Threadneedle Investments EMEA's institutional investment management services for segregated mandates throughout the same period;
- A Subservice Organisation's Statement from CMIA prepared by management providing an assertion that controls related to the control objectives stated in this report were suitably designed and operated effectively throughout the period 1 October 2022 to 30 September 2023, and that the descriptions in Sections I and II of this report fairly present Columbia Management Investment Advisers, LLC's investment management services throughout the same period;
- A Subservice Organisation's Statement from AMPF prepared by management providing an assertion that controls related to the control objectives stated in this report were suitably designed and operated effectively throughout the period 1 October 2022 to 30 September 2023, and that the descriptions in Sections I and II of this report fairly present Ameriprise Financial, Inc's investment management services throughout the same period;
- A Service Auditor's Report, issued by PwC, which provides an opinion on the fair presentation of Sections I and II, the description of the controls in operation throughout the period 1 October 2022 to 30 September 2023 that are set out in Section II, and the suitability of design and operating effectiveness of these controls during the year ended 30 September 2023;
- Section I containing a description of Columbia Threadneedle Investments EMEA's control environment, including areas of corporate governance and management structure, risk management, human resource management, investment management and client service;
- Section II containing a description of Columbia Threadneedle Investments EMEA's control objectives, the controls in operation throughout the period 1 October 2022 to 30 September 2023, and the results of PwC's Service Auditor testing of the controls;
- Section III containing Columbia Threadneedle Investments EMEA's response to the control exceptions identified by PwC's Service Auditor testing of the controls; and
- Section IV containing additional information provided by the Service Auditor;

What is an ISAE 3402/AAF 01/20 Type II Report and what does it mean for our clients?

ISAE 3402 refers to the International Auditing and Assurance Standards Board's (IAASB) 'International Standard on Assurance

Engagements (ISAE) 3402 'Assurance Reports on Controls at a Service Organisation' established to provide a global framework for Service Auditors to provide a report for use by client entities and their auditors on the controls at a service organisation. AAF 01/20 refers to the Technical Release AAF 01/20 Assurance Reports on Internal Controls of Service Organisations made available to third parties issued by the Institute of Chartered Accountants in England and Wales (ICAEW). To further demonstrate our commitment to our clients, we have adopted dual reporting under both ISAE 3402 and AAF 01/20 for this reporting period, which is consistent with the approach taken in previous reporting periods.

In an ISAE 3402/AAF 01/20 'Type II' engagement, the service auditor examines the service organisation's description of controls and carries out procedures to obtain reasonable assurance on whether:

- The accompanying description fairly presents Columbia Threadneedle Investments EMEA's institutional investment management services for segregated mandates;
- The controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls operated effectively throughout the period, and
- Such controls operated effectively during the period.

Columbia Threadneedle Investments EMEA is committed to ensuring that its control environment is documented in a manner that is both relevant and useful to its clients. In particular, by:

- Helping clients discharge their own risk, control, due diligence and supervisory requirements;
- Providing assurance in respect of Columbia Threadneedle Investments EMEA's controls and operating environment; and
- Helping to increase clients' understanding of the Columbia Threadneedle Investments EMEA business.

Service organisations' management statement on controls at Threadneedle Asset Management Limited and Threadneedle International Limited, together referred to as "Columbia Threadneedle Investments EMEA" (the "Service Organisations")

As Directors of the Service Organisations, we are responsible for the identification of control objectives relating to the provision of institutional investment management services by the Service Organisations and the design, implementation and operation of the Service Organisations' controls to provide reasonable assurance that the control objectives are achieved.

The accompanying description in the Introduction and Scope of the Report section, Sections I and II (the "description") has been prepared for customers who have used the institutional investment management services and their auditors who have a sufficient understanding to consider the description, along with other information including information about controls operated by customers themselves, when assessing the risks of material misstatements of customers' financial statements.

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

The Service Organisations present certain subservice organisations using the inclusive method (the "included Subservice Organisations") as indicated on page 3. The Service Organisations' description includes a description of the included Subservice Organisations' systems that are used by the Service Organisations.

The Service Organisations also use certain carved-out subservice organisations (the "carved-out Subservice Organisations") as indicated on page 3. The description excludes the control objectives and related controls of the carved-out Subservice Organisations.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of the Service Organisations' controls are suitably designed and operating effectively, along with related controls at the Service Organisations. The

description does not extend to controls of the user entities.

We have evaluated the fairness of the description, and the design suitability and operating effectiveness of the Service Organisations' controls having regard to the International Standard on Assurance Engagements 3402 (ISAE 3402), issued by the International Auditing and Assurance Standards Board, the Technical Release AAF 01/20 (AAF 01/20), issued by the Institute of Chartered Accountants in England and Wales and the control objectives for institutional investment management services set out in AAF 01/20, except as stated in the description.

We confirm that:

1. The accompanying description, in the Introduction and Scope of the Report section, Sections I and II, fairly presents the Service Organisations' institutional investment management services, and the services provided to the Service Organisations by the included Subservice Organisations, throughout the period 1 October 2022 to 30 September 2023. The criteria used in making this statement were that the accompanying description:
 - presents how the services were designed and implemented, including:
 - the types of services provided, and as appropriate, the nature of transactions processed;
 - the procedures, within both automated and manual systems, by which customers' transactions were initiated, recorded, processed, corrected as necessary, and transferred to the reports prepared for customers;
 - the related accounting records, supporting information and specific accounts that were used to initiate, record, process and report transactions; this includes the correction of incorrect information and how information is transferred to the reports prepared for customers;
 - the systems which captured and addressed significant events and conditions other than customers' transactions;
 - the process used to prepare reports for customers;
 - relevant control objectives and controls designed to achieve those objectives;

- controls that we assumed, in the design of the system, would be implemented by customers, and which, if necessary to achieve the control objective stated in the accompanying description, are identified in the description along with the specific control objectives that cannot be achieved by ourselves alone; and
- other aspects of our control environment, risk assessment process, information systems (including the related business processes) and communication, control activities and monitoring controls that were relevant to processing and reporting customers' transactions.
- includes relevant details of changes to the systems during the period.
- does not omit or distort information relevant to the scope of the services being described, while acknowledging that the description is prepared to meet the common needs of a broad range of customers and their auditors, and may not, therefore, include every aspect of the services that each individual customer may consider important in its own particular environment.

2. The controls related to the control objectives stated in the accompanying description were suitably designed and operating effectively throughout the period 1 October 2022 to 30 September 2023, if user entities applied the complementary controls assumed in the design of the Service Organisations' controls. The criteria used in making this statement were that:

- the risks that threaten the achievement of the control objectives stated in the description were identified;
- the identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved; and
- the controls were consistently applied as designed, including that manual controls were applied by individuals who have the appropriate competence and authority, throughout the period.

David Logan

David Logan (Dec 19, 2023 12:29 GMT)

David Logan

Director for and on behalf of the Board of Directors

Threadneedle Asset Management Limited and
Threadneedle International Limited
19 December 2023

Management's Statement by management of Columbia Management Investment Advisers, LLC

As Management of Columbia Management Investment Advisers, LLC, service providers to Threadneedle Asset Management Limited and Threadneedle International Limited (together the "Service Organisations"), we are responsible, together with the Service Organisations' directors, for the identification of control objectives relating to the provision of certain middle office in support of the Service Organisations' institutional investment management services. We are also responsible for the design, implementation and operation of the Subservice Organisation's controls to provide reasonable assurance that the middle office and information technology ("IT") control objectives are achieved.

The accompanying description including the middle office and IT services provided to the Service Organisations and the details of the controls have been prepared for customers of the Service Organisations who have used their investment management services and their auditors who have a sufficient understanding to consider the description, along with other information including information about controls operated by customers themselves, when assessing the risks of material misstatements of customers' financial statements.

We have evaluated the fairness of the description and the suitability of the design and operating effectiveness of controls over services provided by the Subservice Organisation to the Service Organisations, having regard to the International Standard on Assurance Engagements 3402 (ISAE 3402), issued by the International Auditing and Assurance Standards Board and the control objectives set out in AAF 01/20, issued by the Institute of Chartered Accountants in England and Wales.

We confirm that:

a) The accompanying description in the Introduction and Scope of the Report section, Sections I and II fairly presents the Subservice Organisation's services provided to the Subservice Organisation's throughout the period from 01 October 2022 to 30 September 2023. The criteria used in making this statement were that the accompanying description:

- i. Presents how the middle office services were designed and implemented, including: the types of services provided, including, support and maintenance, the functions by which access to systems and data was restricted, the degree of systems integrity and resilience commensurate with the nature and confidentiality of the information processed and external threats, the requirements for maintaining and developing systems hardware and software; the means by which recovery from processing interruptions was achieved as necessary; controls that we assumed, in the design of the system, would be implemented by customer, which, if necessary to achieve the control objective stated in the accompanying description, are identified in the description along with the specific control objectives that cannot be achieved by ourselves alone; and other aspects of the control environment, risk assessment process, monitoring and information and communication systems, that were relevant to the control activities.
 - ii. Includes relevant details of changes to the systems and services during the period from 1 October 2022 to 30 September 2023.
 - iii. Does not omit or distort information relevant to the scope of the services being described, while acknowledging that the description is prepared to meet the common needs of a broad range of the Service Organisation's customers and their auditors and may not, therefore, include every aspect of the services that each individual Service Organisation's customer may consider important in its own particular environment.
- b) The controls related to the control objectives stated in the accompanying description were suitably designed and operating effectively throughout the period from 1 October 2022 to 30 September 2023. The criteria used in making this assertion were that:
- i. The risks that threatened achievement of the control objectives stated in the description were identified; and
 - ii. The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated IT control objectives from being achieved; and

- iii. The controls were consistently applied as designed throughout the period noted above.

Michael Clarke

Michael Clarke (Dec 18, 2023 07:37 EST)

Michael Clarke, Senior Vice President
Columbia Management Investment Advisers,
LLC
18 December 2023

Management's Statement by the Directors of Ameriprise Financial, Inc.

As Directors of Ameriprise Financial, Inc. (the Subservice Organisation), a service provider Threadneedle Asset Management Limited and Threadneedle International Limited (together the "Service Organisations"), we are responsible, together with the Service Organisations' directors, for the identification of control objectives relating to the provision of certain technology functions in support of the Service Organisation's institutional investment management services. We are also responsible for the design, implementation and operation of the Subservice Organisation's controls to provide reasonable assurance that the IT control objectives are achieved.

The accompanying description including the IT services provided to the Service Organisation and the details of the IT controls have been prepared for customers of the Service Organisation who have used their investment management services and their auditors who have a sufficient understanding to consider the description, along with other information including information about controls operated by customers themselves, when assessing the risks of material misstatements of customers' financial statements.

We have evaluated the fairness of the description and the suitability of the design and operating effectiveness of controls over services provided by the Subservice Organisation to the Service Organisations, having regard to the International Standard on Assurance Engagements 3402 (ISAE 3402), issued by the International Auditing and Assurance Standards Board and the IT control objectives set out in AAF 01/20, issued by the Institute of Chartered Accountants in England and Wales.

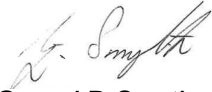
We confirm that:

- a) The accompanying description in the Introduction and Scope of the Report section, Sections I and II fairly presents the Subservice Organisation's IT services provided to the Service Organisations throughout the period from 1 October 2022 to 30 September 2023. The criteria used in making this statement were that the accompanying description:
 - i. Presents how the IT services were designed and implemented, including: the types of services provided, including, IT support and maintenance, the functions by which access to systems and data was

restricted, the degree of systems integrity and resilience commensurate with the nature and confidentiality of the information processed and external threats, the requirements for maintaining and developing systems hardware and software; the means by which recovery from processing interruptions was achieved as necessary; controls that we assumed, in the design of the system, would be implemented by customer, which, if necessary to achieve the control objective stated in the accompanying description, are identified in the description along with the specific control objectives that cannot be achieved by ourselves alone; and other aspects of the IT control environment, risk assessment process, monitoring and information and communication systems, that were relevant to the IT control activities.

- ii. Includes relevant details of changes to the systems and services during the period from 1 October 2022 to 30 September 2023.
 - iii. Does not omit or distort information relevant to the scope of the services being described, while acknowledging that the description is prepared to meet the common needs of a broad range of the Service Organisation's customers and their auditors and may not, therefore, include every aspect of the services that each individual Service Organisations customer may consider important in its own particular environment.
- b. The controls related to the IT control objectives stated in the accompanying description were suitably designed and operating effectively throughout the period from 1 October 2022 to 31 September 2023. The criteria used in making this assertion were that:
- i. The risks that threatened achievement of the IT control objectives stated in the description were identified; and
 - ii. The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated IT control objectives from being achieved; and

Unless otherwise stated in the description, the IT controls were consistently applied as designed throughout the period noted above.



Gerard P. Smyth

Executive Vice President, Technology and Chief
Information Officer
18 December 2023



Independent service auditor's assurance report on controls at Threadneedle Asset Management Limited and Threadneedle International Limited (the "Service Organisations")

To the Directors of Threadneedle Asset Management Limited and Threadneedle International Limited

Scope

We have been engaged to report on the Service Organisations' description of its institutional investment management services throughout the period 1 October 2022 to 30 September 2023 in the Introduction and Scope of the Report section, Sections I and II (the "description"), and on the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description. The controls and control objectives included in the description are those that management of the Service Organisations believe are likely to be relevant to user entities' internal control over financial reporting.

The Service Organisations present certain subservice organisations using the inclusive method (the "included Subservice Organisations") as indicated on page 3. The Service Organisations' description includes a description of the included Subservice Organisation's services used by the Service Organisations to provide institutional investment management services to their customers, as well as relevant control objectives and controls of the included Subservice Organisation.

The Service Organisations also present certain subservice organisations using the carved-out method (the "carved-out Subservice Organisations") as indicated on pages 3 and 4. The description excludes the control objectives and related controls of the carved-out Subservice Organisations. Our examination did not extend to controls of the carved-out Subservice Organisations.

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

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

Our independence and quality control

In carrying out our work, we complied with the Institute of Chartered Accountants in England and Wales (ICAEW) Code of Ethics, which includes independence and other requirements founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour, that are at least as demanding as the applicable provisions of the IESBA Code of Ethics. We also apply International Standard on Quality Management (UK) 1 and accordingly maintain a comprehensive system of quality management including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

The Service Organisations' and the included Subservice Organisations' responsibilities

The Service Organisations and the included Subservice Organisations (where specified) are responsible for: preparing the description in the Introduction and Scope of the Report section, Sections I and II and the accompanying management statements set out on pages 6 to 11, including the completeness, accuracy and method of presentation of the description and the management

PricewaterhouseCoopers LLP, 7 More London Riverside, London, SE1 2RT
T: +44 (0) 20 7583 5000, F: +44 (0) 20 7212 7500, www.pwc.co.uk

PricewaterhouseCoopers LLP is a limited liability partnership registered in England with registered number OC303525. The registered office of PricewaterhouseCoopers LLP is 1 Embankment Place, London WC2N 6RH. PricewaterhouseCoopers LLP is authorised and regulated by the Financial Services Authority for designated investment business.

statements; providing the institutional investment management services covered by the description; specifying the criteria and stating them in the description; identifying the risks that threaten the achievement of the control objectives; and designing, implementing and effectively operating controls to achieve the stated control objectives.

The control objectives stated in the description in the Introduction and Scope of the Report section, Sections I and II are those specified by the Service Organisations as set out in the ICAEW Technical Release AAF 01/20, except where stated otherwise. Management remains solely responsible for determining the suitability of the control objectives to address the needs of intended users.

Service auditor's responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in that description based on our procedures. We conducted our engagement in accordance with International Standards on Assurance Engagements 3402 "Assurance Reports on Controls at a Service Organization" with regards to ICAEW Technical Release AAF 01/20. Those standards and guidance require that we 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. An assurance engagement to report on the description, design and operating effectiveness of controls at a service organisation involves:

- performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of those controls to achieve the related control objectives stated in the description based on the criteria in the management statements on pages 6 to 11;
- 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;
- testing the operating effectiveness of those controls we consider necessary to provide reasonable assurance that the related control objectives stated in the description were achieved; and
- evaluating the overall presentation of the description, suitability of the control objectives stated in the description, and suitability of the criteria specified by the Service Organisations and the included Subservice Organisations in their management statements on pages 6 to 11.

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

Inherent limitations

The Service Organisations' and the included Subservice Organisations' description is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of the Service Organisations' institutional investment management services, or the services provided to the Service Organisations by the included Subservice Organisations, that each individual customer may consider important in its own particular environment. Also, because of their nature, controls at a service organisation or included subservice organisation may not prevent or detect and correct all errors or omissions in processing or reporting transactions. Our opinion is based on historical information and the projection to future periods of any evaluation of the fairness of the presentation of the description, or conclusions 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 described in the Service Organisations' and the included Subservice Organisations' management statements on pages 6 to 11:

- the description in the Introduction and Scope of the Report section, Sections I and II fairly presents the Service Organisations' institutional investment management services, and the services provided by the included Subservice Organisations to the Service Organisations, as designed and implemented throughout the period 1 October 2022 to 30 September 2023;

- the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls operated effectively throughout the period 1 October 2022 to 30 September 2023 and the user entities applied the complementary controls referred to in the scope paragraph of this assurance report; and
- the controls tested, which, together with the complementary user entity controls referred to in the scope paragraph of this assurance report, if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period 1 October 2022 to 30 September 2023.

Description of tests of controls

The specific controls tested and the nature, timing and results of those tests are detailed Section II.

Other information

The information included in Section III is presented by the Service Organisations and the included Subservice Organisations to provide additional information and is not part of the Service Organisations' description of controls that may be relevant to customers' internal control as it relates to an audit of financial statements. Such information has not been subjected to the procedures applied in the examination of the description of the Service Organisations, related to the institutional investment management services, and accordingly, we express no opinion on it.

Intended users and purpose

This report and the description of tests of controls and results thereof Section II are intended solely for the use of the Service Organisations and solely for the purpose of reporting on the controls of the Service Organisations and the included Subservice Organisations, in accordance with the terms of our engagement letter dated 12 June 2023 (the "agreement").

Our report must not be recited or referred to in whole or in part in any other document nor made available, copied or recited to any other party, in any circumstances, without our express prior written permission. Subject to the terms of the agreement, we permit the disclosure of this report, in full only, including the description of tests of controls and results thereof by the Service Organisations at their discretion to customers using their institutional investment management services and to the auditors of such customers, to enable customers and their auditors to verify that a service auditor's report has been commissioned by the Service Organisations and issued in connection with the controls of the Service Organisations and the included Subservice Organisations, and without assuming or accepting any responsibility or liability to customers or their auditors on our part, save where terms are expressly agreed in writing.

We are prepared to extend our assumption of responsibility to those customers of the Service Organisations who first accept in writing the relevant terms of the agreement entered previously with the Service Organisations as if the customer had signed the agreement when originally issued and including the provisions limiting liability contained in the agreement ("Contracted Customers"). This extension will not apply to a customer where we inform that customer, whether before or after the customer accepts the relevant terms of the agreement, that they do not meet our acceptance criteria.

To the fullest extent permitted by law, we do not accept or assume responsibility to anyone other than the Service Organisations and Contracted Customers for our work, for this report or for the opinions we have formed.



PricewaterhouseCoopers LLP
Chartered Accountants
London
19 December 2023

Section I – Description of the Control Environment and Client Control Considerations

1. Global Governance

Columbia Threadneedle Investments believes the following governance arrangements protect and balance the interests of all of our stakeholders, including our end-clients, support the production of relevant management information, effective engagement and challenge at all levels of the business, and promotes a strong culture.

Columbia Threadneedle Investments is structured on the basis of three regions: North America (NA); Europe, Middle East and Africa (EMEA); and Asia Pacific (APAC). Each region has aligned statutory governance and business governance frameworks - statutory focuses on regulatory and legal requirements and reporting, while business governance relates to decision making and day-to-day management.

The Global Governance structure is supported by the Global Heads Group (GHG) and the Global Executive Group (GEG). This provides alignment and coordination across regions and ensures the delivery of global goals and initiatives.

2. Regional Governance

Threadneedle Asset Management UK International Holdings Limited

The main Board in EMEA is that of TAM UK International Holdings Limited (TAM UK Hold Co.), which is the ultimate holding company of the Columbia Threadneedle Investments EMEA group of companies within Ameriprise Financial, Inc. This Board meets quarterly to consider client interests and overall business strategy, set budgets and review forecasts, supervise compliance with regulatory and legal requirements, review results, approve off-budget expenditure, and approve senior level appointments.

There are three committees of TAM UK Hold Co.:

- Audit and Risk Committee;
- Nominating and Governance Committee; and
- Remuneration Committee.

The TAM UK Hold Co. Audit and Risk Committee acts as an advisory committee in order to assist the Board of TAM UK Hold Co. in carrying out its responsibilities as they relate to the risk management, internal control and the conduct of its business across EMEA in accordance with regulation, legislation and business best practice. The committee is also responsible for review and approval of the EMEA Risk Management Framework, in alignment with Ameriprise Financial, Inc's Enterprise Risk Management policies. The Enterprise Risk Management Framework considers all significant strategic, business and operational process risks identified within EMEA and is supported by risk management policies. The TAM UK Hold Co. Audit and Risk Committee comprises six Non-Executive Directors and is chaired by a non-group member. The TAM UK Hold Co. Audit & Risk Committee is authorised to:

- Provide advice, guidance and recommendations to the TAM UK Hold Co. Board and to the Management team of EMEA;
- Approve the EMEA Enterprise Risk Management Framework;
- Investigate any activity within EMEA. It has unrestricted access to all records and staff of EMEA and the external auditors; and
- Obtain outside legal or other independent professional advice and to secure the attendance of outsiders with relevant experience and expertise if it considers this necessary.

The TAM UK Hold Co. Audit and Risk Committee has a direct reporting line to the TAM UK Hold Co. Board and has delegated authority to investigate any activity within EMEA and to seek any information it requires from any employee. The TAM UK Hold Co. Audit and Risk Committee has open access to TAM UK Hold Co's external auditors.

The TAM UK Hold Co. Nominating and Governance Committee is authorised by the TAM UK Hold Co. Board to assume a leadership role in shaping the corporate governance of TAM UK Hold Co. by:

- Identifying, interviewing and recommending new directors to the TAM UK Hold Co. Board and the business;
- Promoting the effective functioning of the TAM UK Hold Co. Board and its committees; and
- Advancing the best interests of TAM UK Hold Co. and its shareholders through the implementation and oversight of sound corporate governance practices, including the resolution of potential conflicts of interests related to other directorships held by Non-Executive Directors and other direct or indirect relationships with other businesses which are wholly or partly in competition with the business carried on by Columbia Threadneedle Investments EMEA.

The TAM UK Hold Co. Nominating and Governance Committee is also authorised to utilise third parties to assist it in the fulfilment of its responsibilities, including identification and screening of director candidates for consideration by the Committee.

The TAM UK Hold Co. Remuneration Committee's primary purpose is to establish and review the philosophy and objectives that will govern the Columbia Threadneedle Investments EMEA Group of companies reward and benefit programme; review and approve reward and benefit plans, policies, and practices, directly oversee the remuneration of EMEA's control functions (Risk, Compliance and Internal Audit), to ensure conflicts of interest are avoided, and oversee and approve EMEA's remuneration including its compliance with relevant regulatory standards.

The TAM UK Hold Co. Board has delegated full authority for the day-to-day running of Columbia Threadneedle Investments EMEA region to its Chief Executive Officer (CEO) David Logan, who joined Columbia Threadneedle Investments EMEA in November 2021. The CEO exercises certain delegated authorities through two separate governance bodies of the EMEA region, the Business Management Committee (BMC) and the Risk and Controls Committee (RCC). These committees are the two senior management and decision-making forums for all activities across the region and ensure that all affairs of the business are cohesively managed and that client interests and potential financial implications are considered by the most senior EMEA management members.

The objective of the BMC is to manage and monitor delivery against strategic and financial plans, including delivery against client needs and interests, and alignment with the global business of Columbia Threadneedle Investments and Ameriprise Financial, Inc. where appropriate.

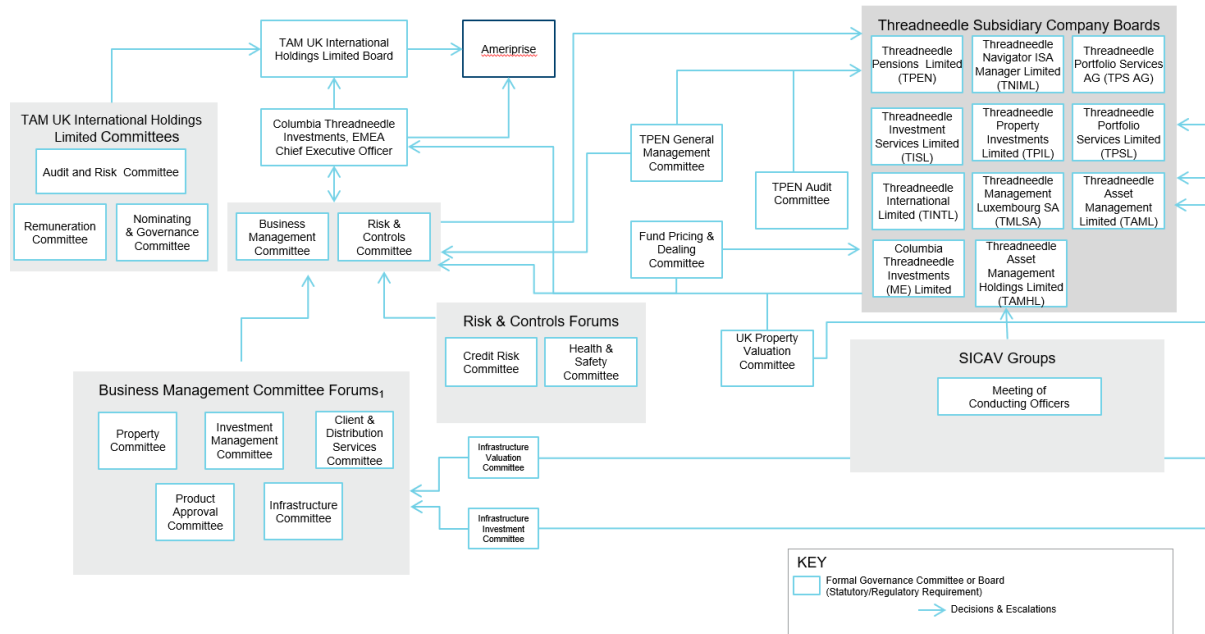
The objective of the EMEA RCC is to manage and mitigate current and prospective risks (including risks to client interests), monitor the effectiveness of controls and consider the capital position and risk appetite of the region.

Decision making, engagement and advocacy

The CEO of Columbia Threadneedle Investments EMEA has delegated certain authorities to functional leadership teams and operating committees.

There are five key sub-committees representing each of the core functions:

- Client and Distribution Services Committee;
- Product Approval Committee;
- Investment Management Committee (IMC);
- Property Committee; and
- Infrastructure Committee.

Figure 1: Statutory Governance Framework and Formal Governance Committees – EMEA

3. Enterprise Risk Management Framework

Introduction

Ameriprise Financial, Inc. has implemented an Enterprise Risk Management (ERM) programme for all of its subsidiaries and operations, including Columbia Threadneedle Investments EMEA. The ERM programme provides a framework for the identification, monitoring and management of risk, including compliance with applicable local regulatory requirements and expectations. It is designed to enable Columbia Threadneedle Investments EMEA to protect the interests of its clients by managing all elements of risk on a forward-looking basis. Ameriprise Financial, Inc. is regulated in many jurisdictions and must ensure it has established and maintains systems and controls appropriate to its businesses. It must establish, implement and maintain adequate risk management policies and procedures.

The guiding principles are:

- Think strategically and creatively to drive innovation in order to best serve our clients and other stakeholders;
- Provide a forward-looking assessment of risk exposure;
- Maintain ERM Policies that are consistent with sound practices for the industry in which it operates, including all applicable regulatory expectations and, which are aligned with those of Ameriprise Financial, Inc.; and
- Failure to act in accordance with the ERM Policies is unacceptable.

Columbia Threadneedle Investments EMEA's policy is that risk management is the primary responsibility of business line management and should be embedded in its various business units and departments. All members of staff have an obligation to be aware of the risks within their processes, understand the controls in place to manage those risks, and report any additional risks or control failures of which they become aware. To this end, a risk management goal is incorporated as part of the performance objectives for all members of staff.

Office of Risk

The EMEA Office of Risk is a group comprising the Heads of Investment Risk, Operational Risk, Compliance, Legal, Internal Audit and Finance, chaired by the Chief Risk Officer (or delegate). The EMEA Office of Risk is designed to help Columbia Threadneedle Investments EMEA make properly informed decisions, by drawing upon the experience and knowledge of a wide group of experienced control functions and risk professionals. The members usually meet at least monthly to discuss current and emerging risk matters and raise items for further debate and challenge at the monthly EMEA RCC meetings. The input of these experts into the risk governance and processes is focused on improving risk outcomes for clients and the business.

Functional Risk Areas

The Operational Risk team establishes the ERM Framework that facilitates a common approach to the identification, assessment and management of risk across Columbia Threadneedle Investments EMEA. The team is also responsible for capturing, analysing and communicating the risk and control profile to the EMEA RCC and other governance bodies.

The Investment Risk team is primarily concerned with market, liquidity and counterparty risks borne by Columbia Threadneedle Investments EMEA's clients. The objectives of investment risk management are to fulfil the fiduciary responsibilities as to the amount and type of market risk taken within the client portfolios, which Columbia Threadneedle Investments EMEA manages.

The Compliance and Internal Audit teams partner with the risk functions in order to implement a combined assurance approach to managing and mitigating risks across Columbia Threadneedle Investments EMEA. Compliance is also responsible for overseeing regulatory risks, Mandate Compliance and Trade Surveillance.

Risk Appetite Framework

The TAM UK Hold Co. Board has established a Risk Appetite Framework, which expresses the tolerance for risks that it faces, and defines the risks that it is prepared to accept in order to deliver strategic objectives. The TAM UK Hold Co. Board delegates day to day responsibility for reviewing / managing risk appetite to the EMEA RCC, which reviews risk appetite levels against each key risk in the taxonomy on a monthly basis. The TAM UK Hold Co. Board, through its Audit & Risk Committee, receives reporting on the business' performance against its risk appetite at least quarterly. This allows management and the TAM UK Hold Co. Board to monitor exposure to risks and ensure that these remain within tolerance. Should a risk exceed its tolerance thresholds consideration is given to if and/or how to:

- Mitigate the risk where possible;
- Explicitly accept the risk, and consider increasing the risk appetite; or
- Scale down or terminate the activity.

Columbia Threadneedle Investments EMEA employs a range of approaches to monitor and report risks throughout the organisation in the context of the Risk Appetite Framework. These include a risk and control self-assessment process, dashboards to report the status and direction of key risks, a rigorous process to identify, record and resolve operational risk events, and policies and procedures covering risks and processes.

The risk appetite may change as the business evolves. The TAM UK Hold Co. Board, through the Audit & Risk Committee, therefore reviews the Risk Appetite Statement annually, as well as when the risks, or the markets in which it operates, are materially altered.

The Risk Appetite Framework is embedded within Columbia Threadneedle Investments EMEA's core business processes and is used as a tool for decision-making and strategic analysis. All the elements used to monitor and report risks inform one another, leading to a cycle of continuous improvement.

Three Lines of Defence

Columbia Threadneedle Investments EMEA has adopted a “Three Lines of Defence” model, to further embed the risk management framework and corporate values, which can be summarised as follows:

Three Lines of Defence – Roles and Responsibilities	
First Line Business Units	Undertake day-to-day risk management
	Comply with the Risk Management Framework, Policies and Procedures
	Apply internal management controls and improvement actions
Second Line Risk and Compliance	Oversee and challenge risk management in First Line of Defence
	Provide guidance and direction to First Line of Defence
	Develop and communicate the ERM Framework
Third Line Internal Audit	Independent perspective and challenge process
	Reviews and oversees both First and Second Line of Defence

Operational Risk

Operational risk is the risk of loss resulting from internal processes which are inadequate or have failed due to human errors, system failures, or external events. Columbia Threadneedle Investments EMEA is exposed to operational risk as a consequence of its core business activities, and seeks to manage and mitigate operational risk, in order to achieve its corporate objectives and fully comply with all regulatory requirements.

The objectives of the Operational Risk strategy are to:

- Reduce operational errors through continuously improving processes and controls;
- Increase the effectiveness and robustness of processes and controls;
- Provide effective reporting for management to understand and manage operational risk; and
- Encourage a positive and proactive operational risk culture.

This is achieved by:

- Establishing an ERM framework that facilitates a common approach to the identification, assessment and management of risk, in order to identify detrimental impacts to Columbia Threadneedle Investments EMEA and its clients;
- Assisting in managing operational risk to within risk appetite;
- Capturing, analysing and communicating the risk and control profile to the EMEA RCC and other governance bodies, in order to help senior management understand and manage operational and enterprise Risk;
- Embedding and ensuring ownership of operational risk by the first line of defence business units, while providing effective guidance and challenge functions;
- Improving operational risk management processes across Columbia Threadneedle Investments EMEA, including coordinating with Ameriprise’s Operational Risk Management team to seek to ensure consistency;
- Facilitating the completion of the risk and control self-assessments (RCSA) by business units e.g. by providing training and guidance on the method employed to identify, assess and score the RCSA risks; and
- Managing the risk event (REV) process to reduce systemic REVs and losses, and by influencing continuous improvement of processes and controls.

Compliance

The Columbia Threadneedle Investments EMEA Compliance Department is responsible for the oversight of compliance with regulatory requirements and standards for the regulated entities within Columbia Threadneedle Investments EMEA.

The objectives of the Compliance function are to:

- Provide policy advice, guidance and training to assist in managing adherence to compliance responsibilities, including anti-money laundering;
- Oversee compliance arrangements to assess whether appropriate systems, procedures and controls are in place;
- Work with senior management to ensure that they are aware of and that they perform their responsibilities and to seek to ensure there are effective governance arrangements within management processes;
- Oversee regulatory risks including successful liaison with regulators and the management of regulatory risk mitigation programmes;
- Ensure that appropriate remedial action is taken where issues have been identified;
- Oversee and monitor investments of the fund portfolios to ensure investments are compliant with investment guidelines, fund objectives and regulatory rules;
- Undertake ongoing surveillance of front office managing and dealing activities of all front office personnel, through a program of daily, weekly and monthly surveillance activities;
- Provide product governance support and oversight; and
- Approve marketing and client communications.

Internal Audit

The Ameriprise Internal Audit team provides independent assessments of the internal control environment and helps Ameriprise improve operations and accomplish its objectives by bringing a systematic, disciplined and risk-based approach to evaluate and improve the effectiveness of risk management, control and governance processes. Internal Audit executes this scope of work via point-in-time audits, targeted or special reviews, key change initiative audits, consulting and advisory services and continuous evaluation activities.

Through the performance of its work, Internal Audit reviews and evaluates the company's risk management, control and governance processes, as designed and represented by management, to provide reasonable assurance that (1) risks are appropriately identified, measured, monitored and controlled, (2) significant financial, managerial and operating information is accurate, reliable and timely, (3) actions taken by Ameriprise and its employees are in compliance with applicable policies, standards, procedures, laws and regulations, (4) resources are acquired economically, used efficiently and protected adequately, (5) assets and information are safeguarded appropriately, and (6) management maintains a culture that promotes risk awareness, accountability, transparency and response.

4. Information Technology

The infrastructure and applications used by Columbia Threadneedle Investments EMEA are supported by Technology staff located in EMEA, North America and India, together with external third-party vendors. The technology team is responsible for the day-to-day functioning of the technology platforms as well as delivering any new systems or applications, or enhancements to existing systems and applications. This report includes testing of controls carried out by staff in EMEA, North America and India, but excludes the testing of controls undertaken by external third-party vendors where management undertakes a review of critical third-party control reports.

In October 2022 investment accounting for institutional accounts was transitioned from HiPortfolio to Aladdin Accounting. The primary accounting areas covered by the project were:

- Accounting (e.g., booking client-directed cash flows, producing valuations, completing month-end close, processing corporate actions)
- Reconciliations (e.g., custodian cash and positions-to-Aladdin, market values-to-custodians)

The tables below detail the applications relevant to the control objectives included within this report:

Applications managed in EMEA

Application	Function	Relevant Control Objective Category	Hosted
CLAUDE	Custom built web application, used to process cash injections and withdrawals, and unit deals	Authorising and Processing Transactions	Internally Hosted
Commodities Decision Support Tool (DST)	Bespoke developed application for the management of the commodity fund range.	Authorising and Processing Transactions	Internally Hosted
Eagle PACE	Central data warehouse for corporate investment data (including unit prices, FX rates, transaction data, valuations, benchmarks, securities).	Reporting to Clients	Internally Hosted
Revport	Client Fee Billing system	Maintaining Financial and Other Records	Internally Hosted
Tidal	Batch Management system	Information Processing	Internally Hosted
Abinitio	ETL and data integration platform	Information Processing	Internally Hosted
Portware	Execution Management system	Trade Execution	Vendor Hosted
Factset	Investment research and analysing portfolio performance and risk	Information Processing Reporting	Vendor Hosted
Bloomberg BTCA	Transaction Cost Analysis / Best Execution Compliance system (EMEA)	Compliance	Vendor Hosted
TCA Generator	Transaction Cost Analysis / Best Execution Compliance system (NA)	Compliance	Internally Hosted
RADAR	RADAR (Risk Analytics, Data and Reporting)	Information processing and reporting to clients	Internally Hosted

Applications managed in North America (CMIA)

Application	Function	Relevant Control Objective Category	Hosted
Frontier	Automates the reconciliation of asset and holdings information between Columbia Threadneedle Investments and custodian records.	Accepting Clients Transaction Processing Maintaining Financial and Other Records	Vendor Hosted
Aladdin	Vendor ASP application used for equity, fixed income and multi-asset portfolio management, analytics, risk management and trading; as well as Middle Office, trade settlement, corporate actions and security attributes (vendor hosted by BlackRock). This also includes Aladdin Accounting.	Authorising and Processing Transactions Monitoring Compliance Middle and Back Office Accounting and Investment Book of Record	Vendor Hosted
InvestOne	Vendor application used for specialised client reporting, and facilitation of collection of security prices.	Maintaining Financial and Other Records Reporting to Clients	Vendor Hosted
Vermilion Reporting Systems (VRS)	Third party software platform capable of integrating with portfolio accounting systems, security/ portfolio analysis tools and files to produce reports. The platform also features integrated template management, workflow, dashboards and a wide range of output formats.	Reporting to Clients	Vendor Hosted
CTI Data Platform	Automated data asset management solution and provides role based access to data.	Maintaining Financial and Other Records Reporting to Clients	Internally Hosted

Applications managed in North America (AMPF)

Application	Function	Relevant Control Objective Category	Hosted
ServiceNow	ServiceNow is a soft-as-a-service (SaaS) provider of IT service management (ITSM) software. Specifically, it is the ticketing system (used to document access requests, support, problem, or incidents).	Recovery from Processing Interruptions	Vendor Hosted
RSA VIA (Aveksa)	Identity Management & Governance manager provides visibility and control who has access to which applications. Primary application used to perform general and privileged access reviews.	Restricting Access to Systems and Data	Vendor Hosted
GoldenSource Security Master (GSSM)	Application developed by GoldenSource Corporation that maintains security data relevant to the setup and maintenance of securities and the execution of trading activity.	Maintaining Financial and Other Records	Internally Hosted

5. Human Resource Policies and Procedures

Columbia Threadneedle Investments EMEA's resourcing policies and procedures ensure delivery of a robust process whereby only those candidates with the right technical skills and behavioural capability are selected.

The resourcing process includes evaluating a candidate's level of competence in previous roles, and their capability against the Columbia Threadneedle Investments EMEA Values (Client Focus, Excellence, Integrity & Respect) and Global Capabilities. Background screening checks are undertaken in line with industry and regulatory requirements. All new employees are required to undertake to adhere to Columbia Threadneedle Investments EMEAs' Values and Global Code of Conduct.

Development of employees is accomplished through a range of learning solutions. The Learning and Development offering is available to all employees and includes, but is not limited to, classroom-based workshops, which have been mapped to the Values and associated competencies, online learning resources, mandatory e-learning, professional qualifications sponsorship, on-the-job training and mentoring.

Columbia Threadneedle Investments EMEA fosters a performance culture where all employees are open to, and actively seek, performance feedback and coaching from their leader. Employees are rated at mid-year and year-end against pre-defined performance goals and the four core values. Those employees not meeting expectations are supported via a Performance Improvement Plan. This is used to address any concerns and support a sustained and consistent improvement in performance and/or behaviour. If an improvement is not seen, the formal Capability Procedure, which provides the framework for managing capability or underperformance issues in a fair and consistent way, is invoked.

Columbia Threadneedle Investments EMEA is committed to maintaining a safe and secure working environment and expects its employees at all times to act within the law, applicable codes of practice, and to apply the highest possible operating and business ethics in all areas of its activities, and it takes very seriously, failure to do so. Employees are encouraged to report suspected wrongdoing as soon as possible, in the knowledge that their concerns will be taken seriously and investigated as appropriate, and that their confidentiality will be respected.

Each of Columbia Threadneedle Investments EMEA's employees, whatever their role, has a personal obligation to apply the right behaviours and uphold the operating, risk and control frameworks, procedures and standards. The Values and the Global Code of Conduct define what this means in practice.

Finally, Columbia Threadneedle Investments EMEA is committed to treating every individual with dignity, respect and keeping the environment free from discrimination and harassment. The Individual Treatment Policy prohibits any type of inappropriate behaviour, intimidation, harassment or retaliation and details how such behaviour will be dealt with.

Employees are aware of how and to whom they can raise any concerns and that these will be treated with the upmost sensitivity and that Columbia Threadneedle Investments EMEA will carry out an investigation and implement any necessary action as soon as is reasonably practicable.

6. Investment Management Approach

Whilst this report does not cover controls related to the Investment Management decision making process the following section outlines Columbia Threadneedle Investments EMEA's Investment Management philosophy and approach.

Investment Philosophy

Clients can access strong and consistent risk-adjusted returns through:

- An active approach that takes advantage of market inefficiencies;
- Global perspective advantage – the combination of macro and micro insights; and
- Appropriate allocation and management of risk.

Investment Approach

Columbia Threadneedle Investments EMEA are active managers with a global reach and an uncomplicated investment approach: better insights result in better decisions and, in turn, better outcomes for clients. The approach is built on four essential pillars:

1. **Meeting clients' goals:** There is an unwavering focus on helping clients achieve their financial goals, through a diverse range of strategies and solutions which are all focused on generating strong and consistent risk-adjusted returns. Global investment insights, combined with local expertise, are enablers to stay abreast of market trends and developments and help clients navigate current and future challenges.
2. **Research driven results:** Investment teams are informed by shared research across multiple asset classes. Collaborative processes encourage investment teams to debate rigorously and challenge the most compelling ideas, every step of the way.
3. **Autonomy with accountability:** Maintaining a culture of intellectual freedom is an essential component of achieving the goals of clients. Consequently, the environment in investments encourages the portfolio managers to construct portfolios using proven experience and expertise. An added layer of independent oversight provides the highest levels of accountability and transparency for clients.
4. **Risk intelligence:** As active managers, risk management is a key pillar of the investment approach. The investment teams seek to manage this by ensuring that risks taken in portfolios are always appropriate and consistent with clients' investment objectives. While inexorably linked to opportunity, risk is multi-faceted. To secure the benefits of well-managed risk, the investment teams focus on understanding its rapidly evolving nature. The portfolio managers are able to intelligently manage risk by applying global insights and know-how to portfolio management.

Portfolio Oversight

The teams manage portfolios against a variety of benchmarks, and close attention is paid to adherence to client guidelines, risk management, portfolio construction and disciplined investment oversight. The '5P' process (product positioning, investment process, people and resources, performance expectations and measurement, and investment philosophy) is central to each team's investment process. The objective of the '5P' process is to understand and validate each team's investment philosophy and methodologies, and if necessary, to improve and enhance upon them by developing additional tools and processes.

Responsible Investment

Columbia Threadneedle Investments EMEA strive to be responsible stewards of clients' assets, believing that effective stewardship benefits companies, investors and the economy as a whole. Well-governed companies are better positioned to manage the risks and challenges inherent in business and are better able to capture opportunities for growth. The investment teams proactively seek to capture these opportunities to help deliver sustainable growth and returns for clients.

Core investment strengths

The capabilities of the investment teams are carefully created, keeping client needs and requirements in mind. Columbia Threadneedle Investments EMEA offers a range of expertise across the risk/reward spectrum, from traditional long-only investments through to specialist alternative vehicles and investment solutions:

- **Equities** – Columbia Threadneedle EMEA offers global, regional and country specific strategies, investing across the market cap spectrum and with various risk and return objectives. Meeting companies and conducting fundamental research lie at the heart of the approach to equity analysis. Using this approach enables the investment teams to identify companies that can create sustainable long-term value by understanding company business models, finances, competitive pressures and drivers of corporate profitability. Face-to-face meetings also provide an opportunity to question management teams on their future plans and strategies. Combining this bottom-up analysis with thematic insights into markets helps build portfolios that can deliver consistent, long-term outperformance.

- **Fixed Income** – The core expertise covers the traditional asset classes of investment grade credit, high yield credit and government bonds; in addition to having significant expertise in more specialist areas of fixed income, including emerging market debt, securitised debt and social bonds. Fundamental research is paramount in the investment approach. Intensive credit analysis helps pursue sustainable and competitive returns. Fostering a collaborative and interactive environment between analysts and portfolio managers enables the best investment ideas to emerge. Fixed income investing is asymmetric – the upside is limited. The investment teams seek to build portfolios that can maximise return per unit of risk to generate strong, consistent outperformance.
- **Multi-asset** – Multi-asset investing is at the heart of the investment philosophy, with extensive capabilities that cover both fundamental and quantitative based strategies investing in a wide range of asset classes. Multi-asset experts are at the hub of the investment framework, enhanced by specialist investment asset class and market teams. While each investment team follows its own unique process and style, ideas are shared and rigorously challenged across asset classes and geographies. In this way, individual investment teams contribute to and help shape the overall macro and investment outlook for the business. As better-informed investors, the multi-asset teams are well positioned to source the very best ideas which contribute to dynamics of portfolios and deliver better investment outcomes.
- **Commodities** – The dedicated Commodities team offer an actively managed strategy to invest in a diverse global portfolio of commodities to access potential capital growth, portfolio diversification and inflation protection benefits offered by this asset class.

Portfolio managers may use derivatives for investment as well as for efficient portfolio management purposes. Portfolio Managers are required to undergo specific, compulsory training before being able to initiate, execute or approve derivatives transactions. Portfolio Managers are required to affirm that they fully understand the derivative they wish to trade and that the use of the derivative is appropriate for the funds in which they intend to trade.

7. Client Management

Client Management is a vital component of Columbia Threadneedle Investments EMEA's business. Asset management and performance are hugely important, but there must also be clear and effective communication with clients. The Client Take On process is coordinated by the Client Management team, Client Contracting team and Client On-Boarding team, with each client assigned a dedicated Client Manager (CM). The scope of services provided to clients is discussed and reviewed with them on a regular basis, in order to ensure that it continues to provide a high level of satisfaction.

The Client Management Team is responsible for:

- The day-to-day running of the segregated client relationships, working with Relationship Managers/Sales to provide excellent service;
- Handling ad hoc client requests relating to reporting and other required data, responding in a timely and efficient manner;
- Ensuring successful and controlled project management of all change management/transitions, with the Client On-Boarding team, including internal and external coordination;
- Ensuring delivery of the client's reporting requirements;
- Support across the product ranges; and
- Continuously reviewing and introducing enhancements to service standards.

8. Amendments and Exclusions

This report contains amendments to or exclusion of certain illustrative Control Objectives included in the investment management and information technology appendices of Technical Release AAF 01/20 as they either relate to activities not applicable to Columbia Threadneedle Investments EMEA, or to activities that are undertaken by third parties appointed by the portfolios managed by Columbia Threadneedle Investments EMEA, as explained below:

AAF 01/20 Illustrative Control Objective	Threadneedle Control Objective	Reason for Amendment or Exclusion
In-house pooled fund unitholder activity is recorded completely, accurately and in a timely manner.	Excluded from report.	The scope of the Columbia Threadneedle Investments ISAE 3402 / AAF 01/20 excludes the administration of pooled funds.
Pooled funds are priced and administered accurately and in a timely manner.	Excluded from report.	The scope of the Columbia Threadneedle Investments ISAE 3402 / AAF 01/20 excludes pooled funds.
Controls provide reasonable assurance that investments are accurately registered and client money is segregated from that of the investment manager.	Excluded from report.	No client money and no client assets are held by either Threadneedle Asset Management Limited, or Threadneedle International Limited.

9. Complementary User Entity Controls

Introduction

Internal controls in Columbia Threadneedle Investments EMEA are only a part of the controls necessary for an effective control environment with regard to the management of clients' assets. Clients themselves may also need to implement and maintain effective internal controls, known as "Client Controls". The required client controls depend upon the nature of the transactions processed by Columbia Threadneedle Investments EMEA, the degree of interaction of controls between Columbia Threadneedle Investments EMEA and the client, and the terms of agreement with Columbia Threadneedle Investments EMEA. This section highlights those client controls that Columbia Threadneedle Investments EMEA anticipates are present in each client's own environment.

Interface and Communication

While describing the control objectives in Section II of this report, it is assumed that all clients have implemented the control measures described below. Each client must evaluate its own Client Controls to determine if the following procedures, surrounding the interface and communication between Columbia Threadneedle Investments EMEA and their organisation are in place. Columbia Threadneedle Investments EMEA advises every client to check within their own internal procedures that these control measures exist.

The following list addresses those controls surrounding the interface and communication between Columbia Threadneedle Investments EMEA and its clients:

- All requirements regarding asset management services are included in the Investment Management Agreement, which is signed by both the client and Columbia Threadneedle Investments EMEA;
- Clients must provide instructions and information to Columbia Threadneedle Investments EMEA in accordance with the Investment Management Agreement;
- Clients must communicate any changes of individuals authorised to instruct Columbia Threadneedle Investments EMEA on a client's behalf in a timely manner;
- Clients must maintain effective controls to provide assurance that all instructions submitted to Columbia Threadneedle Investments EMEA are appropriately authorised;

- Confirmations and invoices as returned by Columbia Threadneedle Investments EMEA should be compared to their original instructions; with any discrepancies being notified to Columbia Threadneedle Investments EMEA immediately;
- Clients should make a timely comparison of the portfolio composition and the relevant benchmark according to the monthly and quarterly reports provided by Columbia Threadneedle Investments EMEA to their own administration records, to provide assurance that:
 - Trades have been recorded completely and accurately;
 - Security valuations used by Columbia Threadneedle Investments EMEA are reasonable;
 - Fair values used for security valuations where market values are not available are reasonable; and
 - Portfolios are being administered in accordance with the Investment Management Agreement;
- Clients with a responsibility for ensuring that trades executed on their behalf by Columbia Threadneedle Investments EMEA are compliant with their own investment guidelines and restrictions, must monitor Columbia Threadneedle Investments EMEA's investment activity to ensure compliance and communicate breaches as soon as reasonably practicable;
- If deviations between Columbia Threadneedle Investments EMEA's reports and the clients' own administration records appear, written notice should be provided to Columbia Threadneedle Investments EMEA in a timely manner; and
- Clients should review their monthly and quarterly reports on a timely basis and reconcile these to the statements provided by their custodian, and discrepancies should be reported to Columbia Threadneedle Investments EMEA as soon as reasonably practicable.
- The Investor Reporting controls described in Section I and II are only applicable to reports formally agreed in the Investment Management Agreement. Clients should review their agreement with Columbia Threadneedle Investments EMEA to confirm which reports are covered by the controls described in Section I and II.
- In the context of control objective 16, where Columbia Threadneedle Investments EMEA is not responsible for calculating the performance fees invoiced, clients should review their performance fee calculations to ensure they are completely and accurately communicated to Columbia Threadneedle Investments EMEA in a timely manner.

The list of client control considerations presented above does not represent a comprehensive set of all controls that should be employed by client organisations. Other controls may be required at a client organisation depending upon each individual situation. Columbia Threadneedle Investments EMEA assumes that the client organisation and the client organisation's auditors confirm that the above-mentioned client controls are in existence and operating effectively. In order for clients to rely on the controls reported herein, each client must evaluate its own internal control structure to determine if the identified user entity controls are in place.

Section II – Control Objectives, Related Controls and Service Auditor Testing and Results

Accepting Clients

Investment Management Agreements are executed with each institutional segregated client. These are executed at the outset of a relationship and may be amended from time to time. This is managed by the Client Contracting team within EMEA Client Management. These agreements include, among other things, the investment objectives of the client and investment guidelines or restrictions imposed upon the account/fund. New accounts are only opened after the Client On-Boarding team has confirmed that the following required actions have been completed and evidenced: consent from the Portfolio Manager and other relevant departments, agreeing to the client's investment guidelines has been provided via the online E-CAP process; and, Investment Management Agreement (IMA) has been signed by the client and a Columbia Threadneedle Investments EMEA authorised signatory.

Columbia Threadneedle Investments EMEA maintains Anti Money Laundering policies and procedures on its intranet and all staff are required to complete web-based training to maintain awareness of their responsibilities on an annual basis. As part of the account opening process the Client Management team will collate required 'Know Your Client' and 'Anti-Money Laundering' documentation for new clients, in accordance with these guidelines, with formal sign-off to confirm the completeness of the information captured as part of the wider E-CAP sign-off process.

Representatives from Columbia Threadneedle Investments EMEA's Client Contracting, Client Management and Legal departments, with direct input from department subject-matter experts, negotiate contract terms with new clients. Standard contracts include the following key elements: Columbia Threadneedle Investments EMEA's obligations; client obligations; custody of assets; indemnification; compliance issues; representations and warranties; and fees and investment guidelines. Where appropriate, as part of the negotiation, responsibility for the generation of proxy voting instructions is clearly established and documented within the IMA. IMAs are signed by an authorised Columbia Threadneedle Investments EMEA employee and an authorised representative from the client before they are considered valid. Once these agreements have been signed the new account is set up on relevant systems based on information obtained during the onboarding process. The Client Management team monitors progress via sign-off of operational readiness within the Mandate Database, and through completion of a checklist, in collaboration with the Client Onboarding team, which tracks the set-up process to ensure that all required steps have been completed to enable the account to be considered 'live'. The Mandate Database is a system that can hold legal documents relating to funds and clients. The system is also used to facilitate the approval process required for new IMAs or following a change to an existing IMA. Key roles and user groups on the Mandate Database are recertified annually.

Prior to initial funding, a Portfolio Manager is assigned to each new client account based on investment strategy. The Portfolio Manager is responsible for managing the account in accordance with the client's investment objectives, risk tolerance, client investment guidelines and internal guidelines. The Portfolio Manager accepts this responsibility by reviewing the account investment guidelines and signing-off on the online E-CAP process. Once the IMA is executed and the client investment guidelines are committed in writing, the Client Contracting team or the Client Management team forwards all related documents to the Legal team. The Client Management team notifies via email: (a) the Portfolio Manager (b) affected business partners and (c) Compliance of the finalised documentation.

1	Controls provide reasonable assurance that client details, accounts, investment guidelines and restrictions are completely and accurately set up onto relevant systems prior to initiating investment activity.	
	Control Procedure	PwC Testing Procedures and Results
1.1	For new Investment Management Agreements (IMA), operational readiness is evidenced by sign-off from relevant parties in the Mandate Database. A checklist is also completed to track that all necessary client set-up steps including client details, client accounts, set-up on third party systems where applicable, fund data, investment guidelines and restrictions, and funding including in-specie transfer have been performed.	<p>Inspection For a sample of new clients, inspected the email correspondence for evidence that Client Services obtained an operational readiness sign-off before the account went live.</p> <p>No exceptions were identified.</p> <p>Inspection For a sample of new clients, obtained and inspected the checklist to confirm that all necessary client set up steps had been completed.</p> <p>No exceptions were identified.</p>
1.2	Prior to initial investment new IMAs and any amendments to existing IMAs are approved by relevant parties via E-CAP. In addition, for amendments requiring system updates, operational readiness is also evidenced by sign-off from relevant parties in the Mandate Database.	<p>Inspection For a sample of new clients, inspected the Contract Approval Form (E-CAP) email for evidence that the IMA was approved by relevant departments prior to initial investment.</p> <p>No exceptions were identified.</p> <p>Inspection For a sample of amendments to IMAs, inspected the Contract Approval Form (E-CAP) email for evidence of approval by the relevant departments prior to implementation of the change. For amendments requiring system updates, also inspected the email correspondence for evidence that Client Services obtained an operational readiness sign-off before the account went live.</p> <p>No exceptions were identified.</p>

2	Controls provide reasonable assurance that client details, accounts, investment guidelines and restrictions are completely and accurately set up onto relevant systems prior to initiating investment activity.	
	Control Procedure	PwC Testing Procedures and Results
2.1	IMAs are signed off by authorised personnel and the client prior to initial investment. Any changes to existing IMAs are not implemented until they have been agreed by the client and Columbia Threadneedle Investments EMEA in writing.	<p>Inspection For a sample of new clients, confirmed that the IMA was signed by authorised personnel and the client prior to initial investment.</p> <p>No exceptions were identified.</p> <p>Inspection For a sample of amendments to IMAs, inspected the IMAs to confirm that they have been signed by authorised personnel and the client prior to implementation of the change.</p> <p>No exceptions were identified.</p>
2.2	Prior to initial investment, new IMAs and any amendments to existing IMAs are approved by relevant parties via E-CAP. In addition, for amendments requiring system updates, operational readiness is also evidenced by sign-off from relevant parties in the Mandate Database.	<p>Inspection For a sample of new clients, inspected the Contract Approval Form (E-CAP) email for evidence that the IMA was approved by relevant departments prior to initial investment.</p> <p>No exceptions were identified.</p> <p>Inspection For a sample of amendments to IMAs, inspected the Contract Approval Form (E-CAP) email for evidence of approval by the relevant departments prior to implementation of the change. For amendments requiring system updates, also inspected the email correspondence for evidence that Client Services obtained an operational readiness sign-off before the account went live.</p> <p>No exceptions were identified.</p>

Mandates may be funded via cash or in-specie. In the case of cash funding, Client Management send an instruction to the Middle Office, who will authenticate the instruction prior to processing. In the case of in-specie funding, the Client Management team share the stock list with the Middle Office, who undertake a reconciliation at the point of take-on from the previous manager.

Once all documentation is reviewed and the cash and/or securities in kind have been confirmed and received by the Custodian, an 'Accounting Funding' email is sent to appropriate parties within Columbia Threadneedle Investments EMEA and the client as notification that the new account funding is complete.

3	Controls provide reasonable assurance that opening balances for client take-ons, including in-specie transfers, are completely and accurately recorded and communicated to clients.	
	Control Procedure	PwC Testing Procedures and Results
3.1	Prior to the commencement of investment activity in respect of a new client, the Client Services team verify that that they have received an authorised notification of funding from the client in line with the IMA prior to notifying the Fund Manager that they may commence trading.	Inspection For a sample of new clients, inspected the email correspondence for evidence that Client Services obtained an operational readiness sign-off before the account went live. No exceptions were identified.
3.2	Daily Cash and stock reconciliations produced by HSBC and Citi are reviewed by the FA Oversight team to ensure all breaks are being followed up. This will be evidenced by sign-off of the FA Oversight Checklist.	Inspection For a sample of days, inspected the cash and stock reconciliations produced by HSBC to confirm that they were reviewed by the Oversight Team and any discrepancies are researched. No exceptions were identified.
3.3	On a daily basis for internally managed funds, the Operations team reconciles the following transactions to Custodian data: <ul style="list-style-type: none"> ■ All settled securities transactions ■ All settled cash transactions Any discrepancies identified are investigated and resolved in line with policy.	Inspection For a sample of days, inspected completed cash and asset reconciliations to confirm that settled securities transactions and settled cash transactions were reconciled to custodian data and that any discrepancies were researched and resolved. No exceptions were identified. Reperformance For one cash reconciliation report, reperfomed the reconciliation using Aladdin Accounting and custodian data to confirm that the system properly identified trade activity not established and maintained timely, accurately and completely. No exceptions were identified. Reperformance For one asset reconciliation report, reperfomed the reconciliation using Aladdin Accounting and custodian data to confirm that the system properly identified trade activity not established and maintained timely, accurately and completely. No exceptions were identified.

3.4	For new Investment Management Agreements (IMA), operational readiness is evidenced by sign-off from relevant parties in the Mandate Database. A checklist is also completed to track that all necessary client set-up steps, including client details, client accounts, set-up on third party systems where applicable, fund data, investment guidelines and restrictions, and funding including in-specie transfer have been performed.	<p>Inspection</p> <p>For a sample of new clients, inspected the email correspondence for evidence that Client Services obtained an operational readiness sign-off before the account went live.</p> <p>No exceptions were identified.</p> <p>Inspection</p> <p>For a sample of new clients, obtained and inspected the checklist to confirm that all necessary client set up steps had been completed.</p> <p>No exceptions were identified.</p>
3.5	Prior to initial investment, new IMAs and any amendments to existing IMAs are approved by relevant parties via E-CAP. In addition, for amendments requiring system updates, operational readiness is also evidenced by sign-off from relevant parties in the Mandate Database.	<p>Inspection</p> <p>For a sample of new clients, inspected the Contract Approval Form (E-CAP) email for evidence that the IMA was approved by relevant departments prior to initial investment.</p> <p>No exceptions were identified.</p> <p>Inspection</p> <p>For a sample of amendments to IMAs, inspected the Contract Approval Form (E-CAP) email for evidence of approval by the relevant departments prior to implementation of the change. For amendments requiring system updates, also inspected the email correspondence for evidence that Client Services obtained an operational readiness sign-off before the account went live.</p> <p>No exceptions were identified.</p>
3.6	For all in specie transfers, Client Management facilitates/co-ordinates agreement with Transition Managers and Custodians of the list of securities to be transferred prior to transition day. Client Change confirm the processing of the agreed securities on Columbia Threadneedle systems. This is evidenced via email confirmation.	<p>Reliance on Risk and Control Services team</p> <p>For a sample of in specie transfers, inspected the email correspondence to confirm the list of securities was agreed with the Transition Manager/ Custodian prior to the transition day.</p> <p>No exceptions were identified.</p>
3.7	From 1 October 2022 to 31 July 2023, all statements (reports, from 1 August 2023 onwards) are independently reviewed and approved by authorized members of the Client Reporting Team. A report completion checklist is used to review all client investment reports, automated client financial statements and send-on reports for completeness and accuracy. The checklist is subject to a secondary independent review prior to release.	<p>Inspection</p> <p>For a sample of in-scope client statements (reports from 01 August 2023), inspected evidence that they are authorised by members of the Client Reporting Team. Further, inspected the report completion checklist along with evidence of secondary review prior to release.</p> <p>No exceptions were identified.</p>

Authorising and Processing Transactions

Trades are processed within the order management systems, Aladdin and Commodities DST. Only persons approved to authorise and execute investment management transactions are given access to the relevant functionality, which must be approved by the employee's line manager. Access rights are independently administered by a central IT department and there is a system-enforced segregation between persons approved to authorise and execute transactions.

Orders are executed sequentially in accordance with the time of their receipt unless otherwise instructed by the client, the interests of the client require otherwise, or the specifics of the order and the current market conditions make this impracticable. Once executed, trades are automatically allocated within the order management systems in line with the fund manager's original allocation.

The Trade Surveillance Group ("TSG") is responsible for the monitoring and oversight of investment and dealing activities to ensure Columbia Threadneedle Investments EMEA meets its regulatory requirements in respect of best execution, allocations (including amended allocations/partial fills), market abuse, and trading conflicts of interest. The surveillance activities carried out by the TSG include monitoring trading patterns and electronic communications in order to prevent and detect potentially suspicious or fraudulent activities or behaviours. The TSG use data extracted from Aladdin and Bloomberg BTCA functionality to assist with the daily review of executed prices. Any issues identified by TSG's review processes will be escalated to the Head of Trading and/or Compliance as is appropriate. Findings from TSG's best execution monitoring are reported to the Trade Monitoring Advisory Group ("TMAG").

Once the order is authorised by the Portfolio Manager (PM) and in the hands of the Dealer, the PM is unable to make changes (system-controlled). The Dealer does not have system permissions that would allow them to amend the allocations set out by the PM. The only amendment that can be made is if the Dealer executes less than the total order size (partial execution). The dealer is permitted (under policy) to manually reallocate / override the auto-allocation in certain circumstances. Where any allocation of an executed trade for any fund on the order differs by 1%, an exception will be identified on the partial fills report and reviewed by the Trade Surveillance Group to confirm it qualifies as a permitted exception.

TMAG is a formal advisory group to the IMC that meets monthly and is responsible for providing oversight, review and challenge in relation to TSG's monitoring processes, in particular Best Execution and Trading Conflicts of Interest monitoring. In addition, TMAG is responsible for reviewing and providing challenge in relation to monthly Best Execution and Trading Conflicts of Interest Dashboards prior to submission to the IMC. As well as providing oversight in respect of TSG monitoring processes, the TMAG is responsible for review and challenge in relation to quarterly TCA monitoring performed by Equity and Fixed Income Trading and the review of execution (dealing) commissions. The TMAG acts to ensure that any issues identified by TSG's monitoring processes are addressed in an appropriate and timely manner and ensuring that any relevant material issues are escalated to the appropriate Governance forum (including the IMC).

The minutes of all TMAG meetings are provided to the IMC on a monthly basis once approved together with a monthly report summarising findings from Best Execution and Trading Conflicts of Interest monitoring processes inter alia. Any issues for escalation identified at the TMAG meeting will also be reported to the IMC.

4	Controls provide reasonable assurance that investment transactions are authorised, executed and allocated accurately within agreed timescales.	
	Control Procedure	PwC Testing Procedures and Results
4.1	Prior to access being granted by authorised system administrators, requests for new or modified systems access accounts are approved by at least one of the following: the requestor's leader, the Environment Owner, or the Environment Owner's delegate.	Inspection For a sample of new access requests, inspect service request tickets and/or application access forms to confirm that the requests had been granted after receipt of approval by the appropriate line manager and other required parties as per access request policies for individual applications. No exceptions were identified.

<p>4.2</p>	<p>All trades must be subject to 4-eyes review prior to being sent to the Dealing team for execution. Segregation of duties between Portfolio Manager (and Portfolio Manager assistants) and Dealers is system-enforced in Aladdin and Commodities DST.</p>	<p>Reliance on Risk and Control Services team</p> <p>Inspection</p> <p>Inspected the results of management's review of user access profiles for in-scope critical applications to confirm that access review had been approved by the Head of IT Operations or delegate to confirm that access was in line with job responsibilities. Inspected accounts' revocation requests from the recertification review, inspected the application access profiles for in-scope critical applications to confirm that access had been revoked per the environment owner's request.</p> <p>No exceptions were identified.</p> <p>Inspection</p> <p>Inspected the results of business owners' reviews of pre-defined segregation of duties matrices to confirm that they had been reviewed by the Business Owner on an annual basis.</p> <p>No exceptions were identified.</p> <p>Inspection</p> <p>Inspected the application access to Aladdin, and the Commodities DST applications to confirm that the applications were configured to enforce segregation of duties between persons approved to authorise and execute investment transactions.</p> <p>No exceptions were identified.</p> <p>Observation</p> <p>Observed a trade in Aladdin and DST Commodities to confirm that trades must be authorised by a Fund Manager prior to being sent to the Dealing team for execution, and that system-enforced segregation was in place preventing the Fund Manager from executing trades and preventing the dealing team from authorising trades.</p> <p>No exceptions were identified.</p>
-------------------	---	---

4.3	Executed trades are automatically allocated within the firm's dealing systems in line with fund managers' (FMs) original allocation. There are system-enforced controls to prevent overbooking in comparison to the FMs' original order size and the transaction is prevented from moving to executed stage by flagging on the traders/dealers and Front Office Assurance and Oversight dashboard.	<p>Observation</p> <p>Observed the overfill dashboard within Aladdin to confirm that overallocated orders above the Fund Manager's original order size are highlighted and reviewed by the Front Office Assurance team.</p> <p>No exceptions were identified.</p> <p>Observation</p> <p>Observed that executed trades are automatically allocated within the firm's dealing systems in line with fund managers' original allocation.</p> <p>No exceptions were identified.</p>
4.4	On a monthly basis, the Trade Monitoring Advisory Group (TMAG) reviews the results from Best Execution and Amended Allocation monitoring processes performed by the Trade Surveillance Group (TSG), including escalations or trade errors identified by these monitoring processes. Any actions noted are recorded in the meeting minutes and followed up at each subsequent meeting. The minutes of the TMA are submitted to the IMC. (TMAG is a formal advisory group thereof.)	<p>Inspection</p> <p>For a sample of months, inspected evidence that the TSG reported findings from their Best Execution and Amended Allocation monitoring processes to the TMAG and details of any escalations were captured in the minutes of the TMAG.</p> <p>No exceptions were identified.</p>
4.5	On a daily basis, a trading manager will review the trader acting as Portfolio Managers report to validate activity is appropriate.	<p>Inspection</p> <p>For a sample of days, inspected evidence that a trading manager reviewed the trader acting as Portfolio Manager reports to validate activity was appropriate.</p> <p>No exceptions were identified.</p>

The counterparties that Columbia Threadneedle Investments EMEA deal with fall into three categories:

- Tier 1 – FX/Derivatives;
- Tier 2 – Cash Bond/Cash Equity;
- Tier 3 – Cash and Money Market Instrument Issuer.

The Counterparty Credit Risk Team (CCRT) maintains a list of approved counterparties with which the funds are permitted to trade, and a periodic review is undertaken to ensure that these lists remain in line with the limits in the relevant systems. Each new broker/counterparty must be requested on a New Broker Approval Form, which is authorised by the requesting dealer, and undergoes a rigorous due diligence and approval process, prior to approval by the Counterparty Credit Risk Committee, and commencement of trading. Appropriate credit thresholds are approved and set within specific risk appetite guidelines based on the internal risk rating given to the counterparty by the Columbia Threadneedle Counterparty Credit Risk team. The Counterparty Credit Risk Committee approves the Counterparty Credit Management Policy and approves or ratifies the appointment of counterparties from the Approved Broker/Counterparty List. There are system-enforced controls within the order management systems to ensure that transactions can only be booked against approved counterparties/brokers.

5	Controls provide reasonable assurance that transactions are undertaken only with approved counterparties.	
	Control Procedure	PwC Testing Procedures and Results
5.1	New FX/Derivative counterparties (T1) counterparties are approved by two members of the Counterparty Credit Risk Committee after due diligence of the new counterparty has been performed. On confirmation of approval from the Counterparty Credit Risk Committee, email notification is sent to both legal and the CTI Operations Team requesting for documentation set-up with the T1 Counterparty and internal set-up of the counterparty on Aladdin post legal documents in place.	Reliance on Risk and Control Services team Inspection For a sample of new FX/Derivative (T1) counterparty requests, inspected the approved Counterparty Risk Credit Risk Committee minutes and due diligence forms for evidence that due diligence was completed and the brokers were approved by the Counterparty Credit Risk Manager and two other members of the Counterparty Credit Risk Committee before being added to Aladdin. No exceptions were identified.
5.2	New cash bond/cash equity (T2) and new money market instrument (T3) counterparties are approved by two members of the Counterparty Credit Risk Committee after due diligence of the new counterparty has been performed. On confirmation of approval from the Counterparty Credit Risk Committee, email notification is sent to the Columbia Threadneedle Operations Team requesting set-up of the T2/T3 counterparty on Aladdin.	Reliance on Risk and Control Services team Inspection For a sample of new cash bond/cash equity (T2) & new money market instrument (T3) counterparty requests, inspected the approved Counterparty Credit Risk Committee minutes and due diligence forms to confirm that due diligence have been completed and the brokers have been approved appropriately by the Counterparty Credit Risk Manager and two other members of the Counterparty Credit Risk Committee before being added to Aladdin. No exceptions were identified
5.3	On an annual basis, a full reconciliation is completed between Approved Counterparty/Broker lists and the trading systems (T1, T2, T3 brokers). Any exceptions are investigated and resolved.	Reliance on Risk and Control Services team Inspection Inspected evidence to confirm that a reconciliation between the Approved Counterparty/Broker List and the trading systems (T1, T2, T3 brokers) is undertaken annually and any exceptions are investigated and resolved. No exceptions were identified.

5.4	Approved FX/Derivative (T1) & money market instrument (T3) counterparties are periodically reviewed within the time frames detailed within the Counterparty Credit Risk Management Policy (Appendix 4.1). All reviews are approved by two members of the Counterparty Credit Risk Committee.	Reliance on Risk and Control Services team Inspection For a sample of FX/Derivative (T1) & money market instrument (T3) counterparties, inspected broker review forms and Counterparty Credit Risk Committee minutes to confirm they were reviewed in line with policy and approved by the Counterparty Credit Manager and two members of the Counterparty Credit Risk Committee. No exceptions were identified.
5.5	System enforced restrictions within Aladdin provide assurance that transactions can only be booked against counter-parties on the Approved Broker List.	Observation Confirmed through observation that only authorised counterparties were able to be selected when conducting trades within the dealing system. No exceptions were identified.

Columbia Threadneedle Investments EMEA pays for research commission directly, with the Data Vendor & Research Services team maintaining a central record of costs, licensing arrangements and an inventory of data and research services supplied to Columbia Threadneedle Investments EMEA under contract. Reports are produced in relation to Equity Transaction Costs and Fixed Income Turnover, which are used to monitor the costs associated with the trading activity. These costs are reviewed and monitored on a quarterly basis by the Trade Monitoring Advisory Group (TMAG), and by the Investment Management Committee (IMC), which also acts as an escalation route if any concerns are identified by the TMAG.

Equity commission reports are produced and a reasonableness review of the commission rates is completed by a member of Trading the trading team. The source data for these reports is from the Data Lake with automated data quality checks are performed prior to Trading review.

6	Controls provide reasonable assurance that transactions are undertaken only with approved counterparties.	
	Control Procedure	PwC Testing Procedures and Results
6.1	New FX/Derivative counterparties (T1) counterparties are approved by two members of the Counterparty Credit Risk Committee after due diligence of the new counterparty has been performed. On confirmation of approval from the Counterparty Credit Risk Committee, email notification is sent to both legal and the Columbia Threadneedle Operations Team requesting for documentation set-up with the T1 Counterparty and internal set-up of the counterparty on Aladdin post legal documents in place.	Reliance on Risk and Control Services team Inspection For a sample of new FX/Derivative (T1) counterparty requests, inspected the approved Counterparty Risk Credit Risk Committee minutes and due diligence forms for evidence that due diligence was completed and the brokers were approved by the Counterparty Credit Risk Manager and two other members of the Counterparty Credit Risk Committee before being added to Aladdin. No exceptions were identified.

6.2	New cash bond/cash equity (T2) and new money market instrument (T3) counterparties are approved by two members of the Counterparty Credit Risk Committee after due diligence of the new counterparty has been performed. On confirmation of approval from the Counterparty Credit Risk Committee, email notification is sent to the Columbia Threadneedle Operations Team requesting set-up of the T2/T3 counterparty on Aladdin.	<p>Reliance on Risk and Control Services team</p> <p>Inspection</p> <p>For a sample of new cash bond/cash equity (T2) & new money market instrument (T3) counterparty requests, inspected the approved Counterparty Credit Risk Committee minutes and due diligence forms to confirm that due diligence have been completed and the brokers have been approved appropriately by the Counterparty Credit Risk Manager and two other members of the Counterparty Credit Risk Committee before being added to Aladdin.</p> <p>No exceptions were identified.</p>
6.3	Investment Operations personnel confirm that trades are accurately entered into the order management system (Aladdin) prior to market settlement date.	<p>Reliance on Risk and Control Services team</p> <p>Inspection</p> <p>Inspected a sample of electronic confirmation exception reports and manual confirmations and noted that the trade discrepancies were identified and resolved by Investment Operations personnel prior to market settlement date.</p> <p>No exceptions were identified.</p>

The Investment Operations department check that trades are accurately entered into the Aladdin system and monitor the Aladdin dashboards for trade confirmation to confirm the transaction details for each trade that has been placed through the system. Trades are confirmed either over the phone or electronically with the broker, on trade date where possible. Trade details for transactions within Aladdin are sent to custodians via SWIFT message and/or DTC affirmation or via a trade file. The executed transactions flow automatically to our portfolio accounting system, Aladdin Accounting.

A daily reconciliation of holdings between the Aladdin system and the custodian is performed by the account and position management teams. Cash is reconciled between Aladdin and the custodian by the cash management team. Trades are matched on a daily basis and any unmatched reconciling items are cleared or carried forward to the next day until they can be resolved.

Fund managers are required to monitor their portfolios on an ongoing basis to ensure that there are no missing trades, that all cash and FX positions have been appropriately covered, and to provide attestation that their funds have been managed appropriately in line with policy. Their attestation confirms that instruments traded, the quantity traded, and all positions were appropriate by reference to:

- The performance objective, risk profile and investment strategy of the fund;
- The applicable mandate and regulatory restrictions and any relevant client instructions;
- The value at which each trade took place was in line with expectations.

7	Controls provide reasonable assurance that investment and related foreign exchange and cash transactions are completely and accurately recorded and communicated for settlement within agreed timescales.	
	Control Procedure	PwC Testing Procedures and Results
7.1	Daily Cash and stock reconciliations produced by HSBC and Citi are reviewed by the FA Oversight team to ensure all breaks are being followed up. This will be evidenced by sign off of the FA Oversight Checklist.	<p>Inspection For a sample of days, inspected the cash and stock reconciliations produced by HSBC to confirm that they were reviewed by the Oversight Team and any discrepancies are researched.</p> <p>No exceptions were identified.</p>
7.2	On a daily basis, Investment Operations personnel monitor the unit dealing system's (CLAUDE) dashboard to confirm that client subscriptions/redemptions received are loaded into CLAUDE, transmitted automatically to the Aladdin accounting system and Order Management System (Aladdin) and that exceptions have been investigated and resolved in line with policy. Reliance on Risk and Control Services team	<p>Inspection For a sample of days, inspected the CLAUDE dashboard to confirm that capital stock instructions were loaded into the unit dealing system, that exceptions were investigated and resolved in a timely manner.</p> <p>No exceptions were identified.</p>
7.3	<p>On a daily basis for internally managed funds, the Operations team reconciles the following transactions to Custodian data:</p> <ul style="list-style-type: none"> ■ All settled securities transactions ■ All settled cash transactions <p>Any discrepancies identified are investigated and resolved in line with policy.</p>	<p>Inspection For a sample of days, inspected completed cash and asset reconciliations to confirm that settled securities transactions and settled cash transactions were reconciled to custodian data and that any discrepancies were researched and resolved.</p> <p>No exceptions were identified.</p> <p>Reperformance For one cash reconciliation report, reperfomed the reconciliation using Aladdin Accounting and custodian data to confirm that the system properly identified trade activity not established and maintained timely, accurately and completely.</p> <p>No exceptions were identified.</p> <p>Reperformance For one asset reconciliation report, reperfomed the reconciliation using Aladdin Accounting and custodian data to confirm that the system properly identified trade activity not established and maintained timely, accurately and completely.</p> <p>No exceptions were identified.</p>

Corporate Actions (COACs) are events initiated by a company that affects the securities they issue, with the primary purpose of returning profits to shareholders, influencing the share price or aligning the security with corporate restructuring.

Corporate Action event notifications are received daily from custodians via SWIFT messages directly into the Aladdin system, and through receipt of a daily feed from Markit. Non-SWIFT Custodians will email Corporate Action events direct to the Columbia Threadneedle Investments EMEA team and a manual record will be set up and approved in Aladdin if the security is only held by a non-SWIFT Custodian. In addition, the Corporate Actions team operate a backstop control using information from Bloomberg to pick up any short fuse events (those with a short deadline). These daily notifications are reviewed by the Corporate Actions team and approved for processing within Aladdin. Notifications are confirmed to a second source to ensure accuracy, and any discrepancies between the notification and the second source are verified to a third source, when available. Exceptions are followed up with the Custodian prior to processing.

Mandatory Corporate Actions, which include stock dividends, full and partial calls, mergers, spin-offs and exchanges, affect all shareholders and do not require Columbia Threadneedle Investments EMEA to make any investment decisions or elections. Upon receipt, a composite is established in Aladdin, which is aligned with the Custodian and/or third-party event data. The actions are processed on ex-date, effective date or pay date as appropriate or when final terms are available and confirmed by a second source.

Voluntary Corporate Actions require election by the Portfolio Managers. Upon receipt into Aladdin, voluntary corporate actions are released to the Portfolio Manager's Aladdin queue for their election. The Corporate Action team tracks these voluntary Corporate Actions by security, earliest response date and effective dates and co-ordinate responses with the Portfolio Managers, who make the investment decisions supported by the Portfolio Managers Assistants (PMAs). All pending Portfolio Manager instructions are tracked via a dedicated control monitor in Aladdin to ensure receipt prior to the earliest Custodian deadline. Within Aladdin there is a system enforced segregation of duties for preparing and releasing instructions that requires dual levels of authorisation before these can be sent by SWIFT to the Custodian.

Both mandatory and voluntary events are processed in Aladdin via the overnight batch process based on the terms specified in the Aladdin composite record. The results of this will be visible in the system on the relevant effective date, pay date or ex-date.

Daily cash and asset balance reconciliations are performed between Aladdin and Custodian bank records to validate that Corporate Actions have been processed as expected. Any discrepancies are researched and resolved.

8	Controls provide reasonable assurance that corporate actions are processed and recorded completely, accurately and within agreed timescales.	
	Control Procedure	PwC Testing Procedures and Results
8.1	<p>Aladdin automated dashboards display all unelected COACs and the relevant deadline. There is a system-enforced secondary review within Aladdin prior to the submission of each instruction to the Custodian via SWIFT.</p> <p>All voluntary events which are communicated via fax are reviewed and approved by the Corporate Actions team prior to being sent to the Custodian. A COAC Front Sheet is prepared and signed to evidence.</p>	<p>Reliance on Risk and Control Services team</p> <p>Inspection</p> <p>For a sample manual COACs, inspected COAC front sheet to confirm that all manual COACs received via fax are reviewed and approved by the Corporate Action teams prior to being sent to the custodian.</p> <p>No exceptions were identified.</p> <p>Observation</p> <p>Confirmed through observation that there is a system-enforced secondary review within Aladdin prior to the submission of voluntary corporate action instructions to the Custodian via SWIFT.</p> <p>No exceptions were identified.</p>
8.2	<p>All Voluntary Corporate Actions which do not have a standing instruction require a Fund Manager election prior to being sent to the custodian. All elections are received automatically through Aladdin.</p> <p>On a daily basis, the Corporate Actions team reviews all Voluntary COACs in Aladdin without an instruction to ensure that elections are received prior to the relevant deadline. A Daily Control Pack is prepared and signed to evidence the review.</p>	<p>Reliance on Risk and Control Services team</p> <p>Inspection</p> <p>For a sample of days, inspected the daily control pack to confirm that the Corporate Actions team reviews all unelected Voluntary COACs in Aladdin to ensure that elections are received prior to the relevant deadline.</p> <p>No exceptions were identified.</p> <p>Inspection</p> <p>For a sample of voluntary corporate actions, inspect the voluntary corporate actions without a standing instruction report from Aladdin to confirm that the Fund Manager election occurred prior to being sent to the custodian.</p> <p>No exceptions were identified.</p>

8.3	<p>On a daily basis, all Mandatory and Voluntary Corporate Actions are processed by the Corporate Actions team on their relevant Ex Date, Effective Date, or Pay date. Completion of all required tasks is evidenced via a Daily Control Pack.</p>	<p>Reliance on Risk and Control Services team</p> <p>Inspection</p> <p>For a sample of days, inspected daily control pack to confirm that all mandatory and voluntary corporate actions are processed by the corporate actions team on their relevant ex-date/effective date/paydate and subject to secondary review.</p> <p>No exceptions were identified.</p>
8.4	<p>On a daily basis for internally managed funds, the Operations team reconciles the following transactions to Custodian data:</p> <ul style="list-style-type: none"> ■ All settled securities transactions ■ All settled cash transactions <p>Any discrepancies identified are investigated and resolved in a timely manner.</p>	<p>Inspection</p> <p>For a sample of days, inspected completed cash and asset reconciliations to confirm that settled securities transactions and settled cash transactions were reconciled to custodian data and that any discrepancies were researched and resolved.</p> <p>No exceptions were identified.</p> <p>Reperformance</p> <p>For one cash reconciliation report, reperfomed the reconciliation using Aladdin Accounting and custodian data to confirm that the system properly identified trade activity not established and maintained timely, accurately and completely.</p> <p>No exceptions were identified.</p> <p>Reperformance</p> <p>For one asset reconciliation report, reperfomed the reconciliation using Aladdin Accounting and custodian data to confirm that the system properly identified trade activity not established and maintained timely, accurately and completely.</p> <p>No exceptions were identified</p>
8.5	<p>Daily Cash and stock reconciliations produced by HSBC and Citi are reviewed by the FA Oversight team to ensure all breaks are being followed up. This will be evidenced by sign-off of the FA Oversight Checklist.</p>	<p>Inspection</p> <p>For a sample of days, inspected the cash and stock reconciliations produced by HSBC to confirm that they were reviewed by the Oversight Team and any discrepancies are researched.</p> <p>No exceptions were identified.</p>

9	Controls provide reasonable assurance that voluntary corporate actions are authorised.	
	Control Procedure	PwC Testing Procedures and Results
9.1	<p>Aladdin automated dashboards display all unelected COACs and the relevant deadline. There is a system-enforced secondary review within Aladdin prior to the submission of each instruction to the Custodian via SWIFT.</p> <p>All voluntary events which are communicated via fax are reviewed and approved by the Corporate Actions team prior to being sent to the Custodian. A COAC Front Sheet is prepared and signed to evidence.</p>	<p>Reliance on Risk and Control Services team</p> <p>Inspection</p> <p>For a sample manual COACs, inspected COAC front sheet to confirm that all manual COACs received via fax are reviewed and approved by the Corporate Action teams prior to being sent to the custodian</p> <p>No exceptions were identified.</p> <p>Observation</p> <p>Confirmed through observation that there is a system-enforced secondary review within Aladdin prior to the submission of voluntary corporate action instructions to the Custodian via SWIFT.</p> <p>No exceptions were identified.</p>
9.2	<p>All Voluntary Corporate Actions which do not have a standing instruction require a Fund Manager election prior to being sent to the custodian. All elections are received automatically through Aladdin.</p> <p>On a daily basis, the Corporate Actions team reviews all Voluntary COACs in Aladdin without an instruction to ensure that elections are received prior to the relevant deadline. A Daily Control Pack is prepared and signed to evidence the review.</p>	<p>Reliance on Risk and Control Services team</p> <p>Inspection</p> <p>For a sample of days, inspected the daily control pack to confirm that the Corporate Actions team reviews all unelected Voluntary COACs in Aladdin to ensure that elections are received prior to the relevant deadline.</p> <p>No exceptions were identified.</p> <p>Inspection</p> <p>For a sample of voluntary corporate actions, inspect the voluntary corporate actions without a standing instruction report from Aladdin to confirm that the Fund Manager election occurred prior to being sent to the custodian.</p> <p>No exceptions were identified.</p>
9.3	<p>On an annual basis, the Corporate Actions team confirm all current standing instructions with the relevant trading desks. Any remedial actions are taken by the Corporate Actions team. This is reviewed and signed off via checklist. Reliance on Risk and Control Services team</p>	<p>Inspection</p> <p>Inspected standing instructions checklist to confirm that the Corporate Actions team confirmed all current standing instructions with the relevant trading desks and any remedial action was taken, reviewed and signed by the Corporate Actions Team.</p>

From time-to-time, clients will request cash movements in relation to their funds. These are processed through the CLAUDE system, by Investment Operations. If cash movements are a regular feature of a portfolio, arrangements are put in place whereby clients notify Columbia Threadneedle of cash movements which are loaded to CLAUDE by Investment Operations. In the case of ad-hoc instructions to withdraw cash from funds, the Client Services team authenticate the client instruction to ensure that it has been appropriately authorised before passing the instruction through email for processing by Middle Office.

10	Controls provide reasonable assurance that client new monies and withdrawals are identified, processed, reported and recorded completely and accurately; withdrawals are appropriately authorised.	
	Control Procedure	PwC Testing Procedures and Results
10.1	Ad-hoc client instructions in respect of withdrawals are independently checked by Client Services to ensure they are appropriately authorised, a 4-eye review of the Cash Advice Form is performed and communicated by email to appropriate stakeholders including Operations and the Front Office.	Inspection For a sample of withdrawals from segregated accounts, inspected the emails to confirm that they were independently checked and communicated to appropriate stakeholders. No exceptions were identified.
10.2	On a daily basis, Investment Operations personnel monitor the unit dealing system's (CLAUDE) dashboard to confirm that Client subscriptions/redemptions received are loaded into CLAUDE, transmitted automatically to the Aladdin Accounting system and Aladdin (Order Management System) and that exceptions have been investigated and resolved in line with policy.	Inspection For a sample of days, inspected the CLAUDE dashboard to confirm that capital stock instructions were loaded into the unit dealing system, that exceptions were investigated and resolved in a timely manner. No exceptions were identified.
10.3	Daily Cash and stock reconciliations produced by HSBC and Citi are reviewed by the FA Oversight team to ensure all breaks are being followed up. This will be evidenced by sign off of the FA Oversight Checklist.	Inspection For a sample of days, inspected the cash and stock reconciliations produced by HSBC to confirm that they were reviewed by the Oversight Team and any discrepancies are researched. No exceptions were identified.

10.4	<p>On a daily basis for internally managed funds, the Operations team reconciles the following transactions to Custodian data:</p> <ul style="list-style-type: none"> ■ All settled securities transactions ■ All settled cash transactions <p>Any discrepancies identified are investigated and resolved in line with policy.</p>	<p>Inspection</p> <p>For a sample of days, inspected completed cash and asset reconciliations to confirm that settled securities transactions and settled cash transactions were reconciled to custodian data and that any discrepancies were researched and resolved.</p> <p>No exceptions were identified.</p> <p>Reperformance</p> <p>For one cash reconciliation report, reperfomed the reconciliation using Aladdin Accounting and custodian data to confirm that the system properly identified trade activity not established and maintained timely, accurately and completely.</p> <p>No exceptions were identified.</p> <p>Reperformance</p> <p>For one asset reconciliation report, reperfomed the reconciliation using Aladdin Accounting and custodian data to confirm that the system properly identified trade activity not established and maintained timely, accurately and completely.</p> <p>No exceptions were identified.</p>
------	--	--

Maintenance of Financial and Other Records

New securities and changes to existing securities executed by Columbia Threadneedle Investments EMEA are communicated by other departments (e.g., Front Office, Compliance, Corp Actions etc.) to the Securities Data Management ("SMDM") Team who are responsible for ensuring they are set up in Aladdin. Securities are created directly within Aladdin either by a Reuters feed or manually by SMDM; Traded and benchmark security data is then fed downstream to GoldenSource Security Master.

The Aladdin Accounting System uses the security data in the Aladdin database added either by the Refinitiv data feed or manually added by the data team. The set-up of new and amended security reference data is subject to independent checks. Data is reviewed on the day of set-up to ensure the security's specific attributes have been established accurately and completely on the Aladdin system, and any discrepancies or missing information are resolved.

Some securities are manually created. These are checked at the point of set-up and the daily controls around the attributes will operate to ensure that these have been set up correctly. An automated feed from the GoldenSource Security Master is transmitted to the Aladdin system at the point of set-up, which updates key security information in the Security Master file. For certain attributes, an automated feed is sent to Aladdin and when there are changes to these attributes, they are reviewed and checked daily.

11	Controls provide reasonable assurance that new security master data and changes to existing security master data are authorised and recorded completely and accurately.	
	Control Procedure	PwC Testing Procedures and Results
11.1	Daily Cash and stock reconciliations produced by HSBC and Citi are reviewed by the FA Oversight team to ensure all breaks are being followed up. This will be evidenced by sign off of the FA Oversight Checklist.	Inspection For a sample of days, inspected the cash and stock reconciliations produced by HSBC to confirm that they were reviewed by the Oversight Team and any discrepancies are researched. No exceptions were identified.
11.2	On a daily basis for internally managed funds, the Operations team reconciles the following transactions to Custodian data: <ul style="list-style-type: none"> ■ All settled securities transactions ■ All settled cash transactions Any discrepancies identified are investigated and resolved in line with policy.	Inspection For a sample of days, inspected completed cash and asset reconciliations to confirm that settled securities transactions and settled cash transactions were reconciled to custodian data and that any discrepancies were researched and resolved. No exceptions were identified. Reperformance For one cash reconciliation report, reperfomed the reconciliation using Aladdin Accounting and custodian data to confirm that the system properly identified trade activity not established and maintained timely, accurately and completely. No exceptions were identified. Reperformance For one asset reconciliation report, reperfomed the reconciliation using Aladdin Accounting and custodian data to confirm that the system properly identified trade activity not established and maintained timely, accurately and completely. No exceptions were identified.
11.3	New and unreviewed securities are set up in Aladdin and reviewed on the day of set-up by the Information Management team using the BAITS tool, fed by Bloomberg, to identify any differences. Any exceptions are investigated and the required updates are entered into Aladdin. A variance check is subsequently performed between Aladdin and BAITS to identify and resolve any further exceptions. Pega requests are closed once all checks have been completed.	Reperformance For a sample of securities, agreed key security attributes from system support files to independent third-party source documentation to determine whether the securities were set up or modified accurately. Further, if discrepancies were identified, reperfomed management's investigation to determine if the discrepancies were researched and resolved. No exceptions noted.

11.4	The Information Management team reviews the End of Day Data Management (DM) Check Report twice a day to identify any missing or inconsistent data elements associated with a security. Any exceptions are investigated and resolved. The Pega task is completed once all exceptions have been actioned.	<p>Inspection</p> <p>For a sample of days, inspected the daily End of Day DM Check Report and Pega audit trail, to confirm all missing or inconsistent data elements have been researched and resolved.</p> <p>No exceptions were identified.</p> <p>Reperformance</p> <p>For a sample of securities, agreed key security attributes from system support files to independent third-party source documentation to determine whether the securities were set up or modified accurately.</p> <p>Reperformance</p> <p>For a sample of new securities, agreed key security attributes from InvestOne to independent third-party source documentation to determine whether the securities were set up accurately.</p>
11.5	The Information Management team performs a 4-eyes check of the front-office's request for a new issue security that is not currently live in the market to be set up against what is entered into Aladdin to ensure the attributes keyed are consistent. Any discrepancies are updated before the new issue is approved, and review confirmation recorded, in Aladdin. Completion of the set-up and 4 eyes check is recorded in Pega by the two individuals completing the tasks.	<p>Inspection</p> <p>For a sample of new issues, inspected audit trail of Pega workflow and Aladdin review confirmation, to confirm independent checks have been completed and recorded in Pega and any discrepancies researched and resolved, prior to review confirmation and new issue approval in Aladdin.</p> <p>No exceptions were identified</p>
11.6	On a daily basis, the Information Management team reviews and resolves data quality exceptions from GoldenSource via IDQ through Pega. The resolved exceptions are commented and closed in Pega. A new exception will be created the following day if not all exceptions are resolved.	<p>Inspection</p> <p>For a sample of days, inspected the information management team's review of data quality exceptions to determine that the review was performed and that exceptions are researched and resolved in Pega in a timely manner.</p> <p>No exceptions were identified</p>

On the ex-dividend date, dividends, dividend withholding tax for foreign security holdings, and income accruals are automatically calculated in the administration system for any portfolio holding the security. The entitlement is automatically loaded into Aladdin Accounting on the ex-dividend date to ensure income is accrued for all authorised fund valuations for the day.

Exception reports identify income entitlement activity not posted through the automated batch process. Exceptions are researched and resolved and manually updated in the system.

Daily cash reconciliations are performed between settled cash transactions and custodian cash transactions to validate that interest and dividend income recorded to the client accounts match the actual amounts in the custodian records. Unmatched items are investigated and resolved.

On a periodic basis, the tax rates applicable to dividends across all fund types are reviewed in Aladdin Accounting. This is to ensure that the ongoing tax and reclaimable rates are accurately reflected within the accounting system.

Upon payment of a tax reclaim receipt, the cash is applied directly to the fund referencing the details of the original dividend to which the reclaim relates.

When reviewing reconciliations provided by HSBC and Citi, the Oversight Team will review to ensure that any challenged reclaims received and visible on the cash reconciliations are valid, posted and cleared as soon as possible. This review is done by comparison to Withholding Tax Reclaim Reconciliations that are received from suppliers and the review of the Cash reconciliations themselves.

12	Controls provide reasonable assurance that investment income and related tax reclaims are completely and accurately recorded in the proper period.	
	Control Procedure	PwC Testing Procedures and Results
12.1	Weekly Income reconciliations produced by HSBC are reviewed by the FA Oversight team to ensure all breaks are being followed up. This is evidenced by sign off of the FA Oversight Checklist.	<p>Reliance on Risk and Control Services team Inspection</p> <p>For a sample of weeks, inspected the outstanding dividends report from HSBC to confirm that it was reviewed by the Threadneedle's Oversight Team. Any issues noted are discussed with HSBC and resolved in a timely manner.</p> <p>No exceptions were identified.</p>
12.2	Daily Cash and stock reconciliations produced by HSBC and Citi are reviewed by the FA Oversight team to ensure all breaks are being followed up. This will be evidenced by sign off of the FA Oversight Checklist.	<p>Inspection</p> <p>For a sample of days, inspected the cash and stock reconciliations produced by HSBC to confirm that they were reviewed by the Oversight Team and any discrepancies are researched.</p> <p>No exceptions were identified</p>
12.3	<p>On a daily basis for internally managed funds, the Operations team reconciles the following transactions to Custodian data:</p> <ul style="list-style-type: none"> ■ All settled securities transactions ■ All settled cash transactions (including tax reclaims) <p>Any discrepancies identified are investigated and resolved in line with policy.</p>	<p>Inspection</p> <p>For a sample of days, inspected completed cash and asset reconciliations to confirm that settled securities transactions and settled cash transactions were reconciled to custodian data and that any discrepancies were researched and resolved.</p> <p>No exceptions were identified.</p> <p>Reperformance</p> <p>For one cash reconciliation report, reperfomed the reconciliation using Aladdin Accounting and custodian data to confirm that the system properly identified trade activity not established and maintained timely, accurately and completely.</p> <p>No exceptions were identified.</p> <p>Reperformance</p> <p>For one asset reconciliation report, reperfomed the reconciliation using Aladdin Accounting and custodian data to confirm that the system properly identified trade activity not established and maintained timely, accurately and completely.</p> <p>No exceptions were identified.</p>

12.4	On a daily basis, the Investment Accounting team completes a checklist to confirm that investment income has been processed accurately by validating it against an independent market data source. The data is updated through electronic transmissions and reviewed for reasonableness, and any exceptions are investigated and resolved.	Reliance on Risk and Control Services team Inspection For a sample of days, inspected the reconciliation between Aladdin and independent market data source, to confirm that Ex Date, Pay Date, Currency and Rate had been correctly captured and any exceptions identified, annotated and resolved. No exceptions were identified.
------	--	--

Day-to-day responsibility for administering pricing is undertaken by CMIA's Global Pricing Team (GPT), who use authorised vendors to price securities, foreign exchange rates and derivatives including Bloomberg; ICE; JP Morgan Pricing Direct; Refinitiv; and Markit. Prices are received daily via automatic feeds, vendor emails or vendor websites and are used to update the current day's market values.

Securities that do not have prices available from these vendors are priced manually by GPT on a daily basis. Fair value pricing methods or quotations received from brokers are used when vendor prices cannot be obtained. Once all positions are priced, price exception and variance reports are generated. The reports identify securities where the change in value from the previous day exceeds a specified tolerance; prices have not changed for a specified period of time; prices are missing or prices are set to zero. GPT managers and analysts review generated reports and clear exceptions. In instances where the GPT managers or Investment Management professionals do not concur with a price provided by a vendor, a price challenge is initiated with the vendor with input from the appropriate trading desk as needed. The Aladdin Accounting system automatically updates portfolios with the price and foreign exchange rate data. For securities where BlackRock does not rely on the CMIA price, a pricing analyst compares the price from CMIA authorised sources to the BlackRock price. Variances exceeding a defined threshold are researched and resolved.

For portfolios administered by HSBC and Citi, security pricing is performed by the outsourced service provider with oversight performed by Columbia Threadneedle's third-party oversight team.

13	Controls provide reasonable assurance that investments with observable prices are accurately valued using current prices obtained from independent external pricing sources.	
	Control Procedure	PwC Testing Procedures and Results
13.1	On a weekly basis, TSG reviews comparable quotes obtained by the Dealers for a sample of non-exchange trades in order to confirm the integrity and accuracy of the quotes recorded in the system for the selected trades based on pricing source (including Bloomberg and / or telephone calls). Any discrepancies are reviewed by TSG. Findings from this review are reported to the TMAG on a monthly basis. Details of any escalations will be captured in the minutes of the TMAG.	Inspection For a sample of weeks, inspected reports to confirm that the TSG performed a review of comparable quotes for a sample of non-exchange trades, and followed up on any discrepancies. No exceptions were identified.

13.2	Security prices are obtained daily from authorised pricing sources. The pricing analyst reviews price variances exceeding a specified tolerance. Reports evidencing the review and resolution are secondary reviewed/initialled by pricing manager.	<p>Inspection</p> <p>For a sample of days, the Daily Security Price Exceptions Summary report was reviewed for variations by a pricing analyst and prices were updated based on information received from authorised sources. Verify the reports have been reviewed signed of (initialled) by pricing management.</p> <p>No exceptions were identified.</p>
13.3	For securities where BlackRock does not rely on the CMIA price, a pricing analyst compares the price from CMIA authorised sources to the BlackRock price. Variances exceeding a defined threshold are researched and resolved. Reports evidencing the review and resolution are secondary reviewed/initialled by the pricing manager.	<p>Inspection</p> <p>For a sample of days, inspected evidence that pricing analyst compared prices between Authorised Source and BlackRock. Verify that the analyst has inspected, researched, and resolved all variances exceeding defined thresholds. Verify that the analyst's work has gone through secondary review.</p> <p>No exceptions were identified.</p>
13.4	Annual ISAE 3402 (or equivalent) Internal Control Reports produced by HSBC and Citi are reviewed by the FA Oversight team at the control objective level, evaluating identified exceptions and user considerations. Where the third- party management response is insufficient, exceptions and qualifications in the reports are escalated to the relationship manager for resolution and/or risk acceptance. Escalation of qualifications for review and resolution is evidenced in the CAR meeting minutes.	<p>Reliance on Risk and Control Services team</p> <p>Inspection</p> <p>For a sample of third party service provider Internal Controls Reports, inspected the review to confirm that Management had reviewed the report at the control objective level, evaluated identified exceptions and evaluated user control considerations, and that exceptions were escalated to the relationship manager for resolution where required.</p> <p>No exceptions were identified.</p> <p>Inspection</p> <p>Inspected CAR meeting minutes for evidence that qualifications were escalated for review and resolution.</p> <p>No exceptions were identified.</p>

13.5	<p>Monthly Service Review Meetings are held with Citi and HSBC to review key performance indicators reflecting agreed service standards and discuss operational issues and the overall effectiveness of the relationship.</p> <p>Key issues are minuted and reviewed for progress at the following meeting to ensure that service levels are maintained.</p>	<p>Reliance on Risk and Control Services team</p> <p>Inspection</p> <p>For a sample of months and quarters, inspected meeting minutes to confirm that Monthly Oversight Meetings were held with the third party service providers and that KPIs were reviewed and key issues were discussed. In addition, inspected the meeting minutes to confirm that key issues are reviewed for progress at the following meeting.</p> <p>No exceptions were identified.</p>
13.6	<p>Missing prices in the portfolio accounting system are reviewed daily by a pricing analyst and updated accordingly based on information received from authorised sources. All pricing updates and overrides are reviewed/initialled by pricing manager.</p>	<p>Inspection</p> <p>For a sample of days, inspected evidence that the Daily Pricing Package was reviewed for variations by a pricing analyst and prices were updated based on information received from authorised sources. Verify that all daily reports, pricing updates and overrides are reviewed/initialled by pricing manager.</p> <p>No exceptions were identified.</p>

The CMIA Valuation Committee is responsible to implement, monitor, oversee and, as relevant, provide assistance in connection with, the valuation of managed assets of Ameriprise Financial, Inc. or its subsidiaries. The Committee has an approved policy for the valuation of portfolio securities. It is CMIA's policy to use third party pricing service(s) and broker-dealers to value the Securities when available and deemed reliable. CMIA is responsible for oversight of such third-party pricing services. CMIA is responsible for monitoring for circumstances that may indicate that prices received do not accurately reflect the current market value of the Securities.

14	<p>Controls provide reasonable assurance that investments without independently available observable prices or prices where only a single pricing source is available are valued according to approved pricing policies and, where necessary, using approved pricing models, assumptions and inputs.</p>	
	Control Procedure	PwC Testing Procedures and Results
14.1	<p>Security prices are obtained daily from authorised pricing sources. The pricing analyst reviews price variances exceeding a specified tolerance. Reports evidencing the review and resolution are secondary reviewed/initialled by pricing manager.</p>	<p>Inspection</p> <p>For a sample of days, the Daily Security Price Exceptions Summary report was reviewed for variations by a pricing analyst and prices were updated based on information received from authorised sources. Verify the reports have been reviewed and signed off (initialled) by pricing management.</p> <p>No exceptions were identified.</p>

14.2	For securities where BlackRock does not rely on the CMIA price, a pricing analyst compares the price from CMIA authorised sources to the BlackRock price. Variances exceeding a defined threshold are researched and resolved. Reports evidencing the review and resolution are secondary reviewed/initialled by a pricing manager.	<p>Inspection</p> <p>For a sample of days, inspected evidence that pricing analyst compared prices between Authorised Source and BlackRock. Verify that the analyst has inspected, researched, and resolved all variances exceeding defined thresholds. Verify that the analyst's work has gone through secondary review.</p> <p>No exceptions were identified.</p>
14.3	A Pricing Policy is in place, which sets out the roles and responsibilities for the valuation of portfolio securities. It details the principles in relation to the current pricing sources, verification of pricing data, fair valuation, pricing challenges and price overrides. The Pricing Policy is approved by the CMIA Valuation Committee.	<p>Reliance on Risk and Control Services team</p> <p>Inspection</p> <p>Inspected the pricing policy to verify that it is in place and details roles and responsibilities related to the valuation of portfolio securities, details the principles related to current pricing sources, verification of pricing data, fair valuation, pricing challenges, and pricing overrides. Inspected Valuation Committee meeting minutes to verify that the pricing policy was approved.</p> <p>No exceptions were identified.</p>
14.4	The CMIA Valuation Committee meets on a monthly basis and ad-hoc as required to make decisions on fair value pricing. Actions are recorded in the meeting minutes and followed up at the subsequent meeting.	<p>Reliance on Risk and Control Services team</p> <p>Inspection</p> <p>For a sample of months inspected evidence that the CMIA Valuation Committee took place to make decisions on fair value pricing and actions were recorded and followed up at subsequent meetings.</p> <p>No exceptions were identified.</p>

14.5	<p>Annual ISAE 3402 (or equivalent) Internal Control Reports produced by HSBC and Citi are reviewed by the FA Oversight team at the control objective level, evaluating identified exceptions and user considerations. Where the third-party management response is insufficient, exceptions and qualifications in the reports are escalated to the relationship manager for resolution and/or risk acceptance.</p>	<p>Reliance on Risk and Control Services team</p> <p>Inspection</p> <p>For a sample of third party service provider Internal Controls Reports, inspected the review to confirm that Management had reviewed the report at the control objective level, evaluated identified exceptions and evaluated user control considerations, and that exceptions were escalated to the relationship manager for resolution where required.</p> <p>No exceptions were identified.</p> <p>Inspection</p> <p>Inspected CAR meeting minutes for evidence that qualifications were escalated for review and resolution.</p> <p>No exceptions were identified.</p>
14.6	<p>Monthly Service Review Meetings are held with Citi and HSBC to review key performance indicators reflecting agreed service standards and discuss operational issues and the overall effectiveness of the relationship.</p> <p>Key issues are minuted and reviewed for progress at the following meeting to ensure that service levels are maintained.</p>	<p>Reliance on Risk and Control Services team</p> <p>Inspection</p> <p>For a sample of months and quarters, inspected meeting minutes to confirm that Monthly Oversight Meetings were held with the third-party service providers and that KPIs were reviewed and key issues were discussed. In addition, inspected the meeting minutes to confirm that key issues are reviewed for progress at the following meeting.</p> <p>No exceptions were identified.</p>

Asset holdings and cash are maintained in the Aladdin Accounting system at an individual account level. Cash and cash equivalents are reconciled daily between the Aladdin Accounting system and the custodian bank account for each account. Custodian information is obtained via SWIFT messages or downloaded from the custodian website. A manual daily cash balancing process is used to balance accounts for which custodian, balance or transaction information is unavailable. These accounts are either held by custodians for whom a data link cannot be established or are new accounts for which the data upload process is not yet functional. Identified differences are researched and followed up.

Portfolio positions are reconciled daily between the Aladdin Accounting system and the custodian bank account for each account where portfolio holdings information is available from the custodian. A manual portfolio reconciliation process is used to balance accounts for which custodian holdings information is unavailable.

Management monitors breaks to ensure timely research and resolution of reconciling items. Unmatched balances are researched and resolved by the Reconciliation and Investment Operations team.

15	Controls provide reasonable assurance that cash and investment positions are completely and accurately recorded and reconciled to third party data.	
	Control Procedure	PwC Testing Procedures and Results
15.1	Daily Cash and stock reconciliations produced by HSBC and Citi are reviewed by the FA Oversight team to ensure all breaks are being followed up. This will be evidenced by sign-off of the FA Oversight Checklist.	Inspection For a sample of days, inspected the cash and stock reconciliations produced by HSBC to confirm that they were reviewed by the Oversight Team and any discrepancies are researched. No exceptions were identified.
15.2	On a daily basis for internally managed funds, the Operations team reconciles the following transactions to Custodian data: <ul style="list-style-type: none"> ■ All settled securities transactions ■ All settled cash transactions Any discrepancies identified are investigated and resolved in line with policy.	Inspection For a sample of days, inspected completed cash and asset reconciliations to confirm that settled securities transactions and settled cash transactions were reconciled to custodian data and that any discrepancies were researched and resolved. No exceptions were identified. Reperformance For one cash reconciliation report, reperformed the reconciliation using Aladdin Accounting and custodian data to confirm that the system properly identified trade activity not established and maintained timely, accurately and completely. No exceptions were identified. Reperformance For one asset reconciliation report, reperformed the reconciliation using Aladdin Accounting and custodian data to confirm that the system properly identified trade activity not established and maintained timely, accurately and completely. No exceptions were identified.

Where Columbia Threadneedle Investments EMEA is responsible for the calculation of management and performance fees, the Finance team is responsible for management and performance fee calculations and utilise the billing system Revport for these calculations. To provide assurance in respect of accuracy, each fee is calculated and independently reviewed within Finance, to ensure that the appropriate funds under management position has been applied to the correct fee rate and covers the correct period(s). In completing their review and approval a visual check of the Funds Under Management (FUM) is undertaken to ensure details have been loaded correctly into the Revport system; that the fee scales held in the system are correct and that any movement in fees from the prior period invoice is reasonable relative to any movement in FUM. The FUM values data quality is validated before being calculated by Investor Reporting and subsequently reviewed for accuracy and completeness. Additionally, for performance fees calculated internally, the performance figures used in the calculation are confirmed back to the reviewed and signed off Aladdin or Factset returns as supplied by the Performance Team.

For client-calculated performance fees, the internal calculation is performed as above and then compared to the client's calculation, with any material discrepancies investigated and resolved. Such performance fees are not in scope for this report.

16	Controls provide reasonable assurance that investment management and performance fees and other account expenses are accurately calculated and recorded.	
	Control Procedure	PwC Testing Procedures and Results
16.1	<p>Returns for all portfolios with performance fees are subject to review and sign off by a member of the Performance team on a monthly basis.</p> <p>Current month returns are calculated using Investment Accounting data.</p> <p>Any variances outside of tolerance, 2.5bps for monthly returns, are investigated and resolved prior to release of returns. Variances that cannot be fully resolved and documented prior to release are escalated and may be released on approval of a senior member of the Performance team.</p>	<p>Inspection</p> <p>For a sample of months and returns for portfolios, inspected evidence of review and sign off by a member of the Performance team of current month and cumulative returns calculated using Investment Accounting data. For any variances outside of tolerance, inspected evidence that these were investigated prior to release of returns. Where variances could not be fully resolved and documented prior to release, inspected evidence that these were escalated and released on approval of a senior member of the Performance team.</p> <p>No exceptions were identified.</p>
16.2	<p>On a monthly basis, a member of the Performance team extracts a report from FactSet and reviews current and prior month historical returns from SPAR to verify returns remain accurate and have not been amended in error.</p> <p>The review is performed versus Aladdin for all accounts with performance fees. Any discrepancy noted in historical returns is investigated and resolved prior to the next reporting cycle. When the review is completed, the report is signed off by a second member of the Performance team.</p>	<p>Inspection</p> <p>For a sample of months, inspected evidence that a member of the Performance team reviewed the current and prior month historical returns from FactSet and verified that returns remained accurate and have not been amended in error. Where there were discrepancies noted in historical returns, inspected evidence that these were investigated and resolved prior to the next reporting cycle. Further, inspected evidence that the report was signed off by a second member of the Performance team.</p> <p>No exceptions were identified.</p>
16.3	<p>Source data used for performance fee calculations is reviewed and signed off prior to being released for onward distribution. The 4-eye review is evidenced by e-mail. The review is performed for all accounts with performance fees.</p>	<p>Inspection</p> <p>For a sample of performance fee calculations, inspected email correspondence to confirm that the source data was reviewed and sign off prior to release for onward distribution.</p> <p>No exceptions were identified.</p>

16.4	Finance reviews each management fee calculation to provide assurance that there have been no changes to the calculation methodology. In approving the invoice, the reviewer confirms that the amount is correct and that they have visually checked that the Funds Under Management (FUM) has been loaded correctly, the Fee Scales are correct and the movement in fees from the prior period invoice is reasonable given the movement in FUM. Any discrepancies identified are investigated and resolved in line with policy.	<p>Reliance on Risk and Control Services team</p> <p>Inspection</p> <p>For a sample of invoices, inspected the fee calculation and invoices to confirm that they were reviewed and approved.</p> <p>No exceptions were identified.</p>
16.5	For performance fee invoices issued, Finance review and calculate performance fees to confirm performance fee accuracy. Any discrepancies identified are investigated and resolved in line with policy.	<p>Inspection</p> <p>For a sample of performance fee invoices, inspected the performance fee calculation and invoices to confirm that they were reviewed and calculated.</p> <p>No exceptions were identified.</p> <p>Reperformance</p> <p>For the same sample, reperformed the manual calculation for performance fees using performance data from Factset and FUM from Aladdin Accounting to confirm completeness and accuracy of the calculation of the performance fee on the invoice.</p> <p>No exceptions were identified.</p>
16.6	Revport automatically posts performance and management fees to the ledger. The Revport ledger is reconciled to the group general ledger by the Finance team on a monthly basis. All exceptions are resolved by the Finance team in line with policy.	<p>Reliance on Risk and Control Services team</p> <p>Inspection</p> <p>For a sample of months, inspected the reconciliation of the Revport ledger to the group general ledger by the Finance team to confirm all exceptions are resolved by the Finance team.</p> <p>No exceptions were identified.</p>
16.7	All invoices generated by Revport are approved by a secondary Finance team member. Revport systematically enforces segregation of duties; it is not possible for the preparer of an invoice to also be the approver.	<p>Inspection</p> <p>Inspected the segregation of duties matrix to confirm no individual had both preparer and approver status.</p> <p>No exceptions were identified.</p> <p>Observation</p> <p>Observed the systematically enforced segregation of duties in Revport to confirm that the invoice preparer cannot also approve the invoice.</p> <p>No exceptions were identified.</p>

16.8	A series of automated daily and monthly Data Quality checks ensure population and consistency of key data points. Data Quality checks ensure all accounts are published prior to the FUM calculations running with further checks reconciling total market values in the data sets back to the canonicals in the Data Platform.	Inspection For a sample of months, inspected the DQ system audit report to confirm that any and all failure instances generated an email to control owners via Service Now and that all issues were annotated, investigated and resolved. No exceptions were identified.
16.9	A FUM checklist is run through to review and load the external FUM holdings and movements data into the Data Lake. Automated Data Quality checks are reviewed to ensure data is in a useable state for downstream recipients. The Checklist is subject to a secondary independent review and sign-off.	Inspection For a sample of months, inspected the Report Completion Checklist to confirm that it was subject to a secondary independent review prior to release to Finance. No exceptions were identified.

The Mandate Compliance team is responsible for ensuring that portfolios are managed in accordance with client restrictions set out in the IMA in respect of cash borrowing and cash held on deposit with financial institutions. The Mandate Compliance team uses Aladdin compliance functionality to code and monitor compliance with these restrictions. Where a limit or restriction cannot be monitored automatically by the system, it will be managed via a manual rules test which will prompt the team to run a separate process. Potential breaches of investment guidelines, which are identified post trade, are identified and escalated through the post-trade process. Where it is established that an actual breach has occurred this will be recorded in the Mandate Compliance breach log. Columbia Threadneedle Investments EMEA input active breaches into the global risk management system, MetricStream.

17	Controls provide reasonable assurance that cash is managed with regard to diversification of risk and security of funds.	
	Control Procedure	PwC Testing Procedures and Results
17.1	Manual Rule Tests are set up in Aladdin where mandate restrictions cannot be automatically monitored by the system. Generated alerts are actioned by the Mandate Compliance team, in accordance with the associated manual rule test procedure at the defined interval. Identified exceptions are investigated in line with policy.	Inspection For a sample of manual rule tests, inspected evidence that the manual rule test was actioned by a member of the Mandate Compliance Team and identified exceptions are investigated in line with policy. No exceptions were identified.

17.2	On a daily basis, a member of the Mandate Compliance Team extracts and reviews an end-of-day report from Aladdin containing all live violations and a rationale is added for any alerts which are pending action or are closed without a future test date. This review is evidenced via email sign-off.	<p>Inspection For a sample of days, inspected evidence of the review of the end of day report from Aladdin containing all live violations and confirmed that a rationale was added for any alerts which were pending action or were closed without a future test date and an email was sent to Mandate Compliance team for proof of review.</p> <p>Exceptions noted. Management self-identified two instances during the period where the end of day check (Control 18.6) had not been performed:</p> <ul style="list-style-type: none"> i) End of day review for 9 Feb 23 ii) End of day review for 26 July 2023 (additional MIE communicated to PwC on 10/08/2023) <p>Inspection Confirmed through inspection of one end of day report from Aladdin containing all live violations of manual and automated rules triggered the previous day that the data contained within it completely and accurately reflected the data held on Aladdin.</p> <p>No exceptions were identified.</p>
17.3	On a daily basis, the Mandate Compliance monitoring team are responsible for reviewing all new and repeating alerts generated by the overnight batch process in Aladdin. All new alerts generated (i.e., those alerts which have an age of 1 day) are subject to a second review by another member of the Mandate Compliance monitoring team. Both the first and second review of new alerts are recorded within Aladdin.	<p>Inspection For a sample of new alerts, inspected screenshots from Aladdin to confirm they were subject to a secondary review by a separate senior team member of the Mandate Compliance monitoring team.</p> <p>Exceptions noted.</p> <p>Management self-identified 3 instances during the period where the 4-eyes review of new alerts for the day (had not been performed.</p> <p>Details of missed 4 eyes reviews (exceptions in control 18.7) and the end of day check which failed to identify the issue (exceptions in control 18.6):</p> <ul style="list-style-type: none"> i) 1 new alert on 26 Jan 23 ii) 1 new alert on 20 Mar 23 ii) 1 new alert on 24 May 23

17.4	On a quarterly basis, a review will be completed by a senior member of the Mandate Compliance team to confirm no compliance rules have been mistakenly removed from portfolios by members of the EMEA Mandate Compliance Coding team. The review utilises a report of removed rules provided by BRS. Any issues identified by the review process will be investigated and followed up with the coding analyst if required. Where a rule is identified as having been mistakenly removed, the rule will be reinstated immediately, and a retrospective check performed for the period when the rule was not operating.	<p>Inspection</p> <p>For a sample of quarters, inspected the review of compliance rules to confirm that it was reviewed by a senior member of the Mandate Compliance team and any issues identified are investigated and followed up. Where a rule is mistakenly removed, confirm that the rule is reinstated immediately and a retrospective check performed for the period when the rule was not operating.</p> <p>No exceptions were identified.</p>
------	---	--

Monitoring Compliance

The primary responsibility for investment guideline compliance rests with the Portfolio Management teams. Guidelines are agreed with clients and documented in Investment Management agreements, thereafter they are logged in the Mandate Database that all Portfolio Managers have access to. Portfolio Managers are expected to become thoroughly familiar with their client investment guidelines. In addition, Portfolio Management teams meet on a regular basis to review portfolios, discuss strategies, and review compliance.

The Portfolio Management teams are supported by the Mandate Compliance team. Mandate restrictions and internal control checks are coded into Aladdin to report transactions in unauthorised investments. This ability to assign and amend rule coding is restricted to authorised individuals. Any new users are required to be approved by the Head of Mandate Control and Front Office Advisory, EMEA and Global Front Office Risk and Controls, with access administration performed by a central team supported by BlackRock Solutions.

The Mandate Compliance Team use systems and defined processes to check that portfolios are managed in accordance with relevant client IMA guidelines and regulatory restrictions. The Mandate Compliance Team review all new and amended investment mandates to identify the required rules and restrictions, which they code for automatic monitoring where possible by the order management system, Aladdin. For each fund, hard and soft mandate rules are coded into the systems and trigger automatically on a pre- and post-trade basis acting to prevent and/ or identify any breaches that may occur. A prohibitive hard rule requires an independent approval by Mandate Compliance to override. A soft rule, which typically relates to investment spread and concentration parameters, that may fluctuate based on the day's trading, may be processed by the fund manager, who is required to insert a comment into the system. Where a limit or restriction cannot be monitored automatically by the system or the rule needs to be updated on a regular basis to ensure it remains relevant it is coded as a manual rule test, which creates a prompt to run a separate process or update a parameter in a working automated rule. These manual rule tests comprise a very small percentage of the overall mandate rule population and are designed to prompt staff to perform additional manual checks or agreed procedures on the relevant fund or working rule based on either a pre-determined date or due to a change in the position on a fund.

In addition, the Commodities Decision Support Tool (DST) is used by the Commodities Desk to raise SWAP trades and send these trades to the Dealing Desk. The dealers are able to pick up these trades and send them to market for execution. The DST has only the SWAPs that are permitted by the portfolio, only has authorised counterparties and is only used for the portfolio SXECOM. Aladdin automatically prevents large trades from being executed without further review, and approval by suitable authorised individuals, in line with Columbia Threadneedle Investments EMEA's "Fat Finger Policy". Approval for large trades is provided by authorised Fat Finger approvers. The risk profile of all funds and portfolios is reviewed at Desk Risk meetings, which take place quarterly. Issues raised during these meetings are minuted and incorporated into the review of investment risk performance performed by the Investment Risk Advisory Group (IRAG), with any significant issues noted at these meetings, and monitored until satisfactory resolution. The Investment Management Committee reviews fund performance on a monthly basis, and fixed income and equity twice yearly. The risk

profiles of all funds and portfolios are reviewed quarterly by the respective desk head and Chief Investment Officer. There is independent sign-off within a SharePoint tracker that fund performance has been reviewed and validated.

18	Controls provide reasonable assurance that client investments and cash are managed in accordance with investment objectives and monitored for compliance with investment guidelines and restrictions.	
	Control Procedure	PwC Testing Procedures and Results
18.1	Prior to access being granted by authorised system administrators, requests for new or modified systems access accounts are approved by at least one of the following: the requestor's leader, the Environment Owner, or the Environment Owner's delegate.	Inspection For a sample of new access requests, inspect service request tickets and/or application access forms to confirm that the requests had been granted after receipt of approval by the appropriate line manager and other required parties as per access request policies for individual applications. No exceptions were identified.
18.2	Prior to executing a trade, Aladdin uses Compliance and Investment approval-based rules to automatically notify Fund Managers that an intended order may breach a client's mandate restrictions. Compliance approval rules require independent approval by Mandate Compliance. The Investment approvals are processed by the order raiser (can be PMA or Fund Manager) who are required to insert a comment into the system; these are then authorised by the Fund Manager.	Observation Confirmed through observation that for a rule that requires Mandate Compliance approval, the fund manager was automatically notified that the intended order will breach client's mandate restrictions, and the trade could not be executed by the fund manager without approval by Mandate Compliance. No exceptions were identified. Observation Confirmed through observation that for a rule that requires Investment approval, the fund manager was automatically notified that the intended order will breach client's mandate restrictions and they had to insert comments into the system before he was able to override the notification requiring Investment approval. No exceptions were identified.
18.3	Commodities DST is used for the purpose of commodity swap trading. Only approved indices and counterparties are set up in Commodities DST and cannot be overwritten by Fund Managers or traders.	Observation Observation that investment guidelines and restrictions which are built into DST cannot be overwritten by the Fund Manager. No exceptions were identified.

18.4	On a monthly basis, the Investment Management Committee (IMC) reviews the results of any internal Investment Consultancy team (5P) reviews and reports covering the performance and investment risk of all investment strategies. Any actions noted are recorded in the meeting minutes and followed up at each subsequent meeting.	<p>Reliance on Risk and Control Services team</p> <p>Inspection</p> <p>For a sample of months, inspected meeting pack and minutes to confirm that IMC reviewed any 5P reviews and performance and investment risk reports for investment strategies, and that actions noted are recorded in the meeting minutes and followed up at each subsequent meeting.</p> <p>No exceptions were identified.</p>
18.5	Manual Rule Tests are set up in Aladdin where mandate restrictions cannot be automatically monitored by the system. Generated alerts are actioned by the Mandate Compliance team, in accordance with the associated manual rule test procedure at the defined interval. Identified exceptions are investigated in a timely manner and in line with policy.	<p>Inspection</p> <p>For a sample of manual rule tests, inspected Aladdin to confirm that the manual rule test was investigated by a member of the Mandate Compliance Team in a timely manner and that identified exceptions are investigated in a timely manner.</p> <p>No exceptions were identified.</p>
18.6	On a daily basis, a member of the Mandate Compliance Team extracts and reviews an end-of-day report from Aladdin containing all live violations and a rationale is added for any alerts which are pending action or are closed without a future test date. This review is evidenced via email sign-off.	<p>Inspection</p> <p>For a sample of days, inspected evidence of the review of the end of day report from Aladdin containing all live violations and confirmed that a rationale was added for any alerts which were pending action or were closed without a future test date and an email was sent to Mandate Compliance team for proof of review.</p> <p>Exceptions noted.</p> <p>Management self-identified two instances during the period where the end of day check (Control 18.6) had not been performed:</p> <ul style="list-style-type: none"> i) End of day review for 9 Feb 23 ii) End of day review for 26 July 2023 (additional MIE communicated to PwC on 10/08/2023) <p>Inspection</p> <p>Confirmed through inspection of one end of day report from Aladdin containing all live violations of manual and automated rules triggered the previous day that the data contained within it completely and accurately reflected the data held on Aladdin.</p> <p>No exceptions were identified.</p>

18.7	On a daily basis, the Mandate Compliance monitoring team are responsible for reviewing all new and repeating alerts generated by the overnight batch process in Aladdin. All new alerts generated (i.e., those alerts which have an age of 1 day) are subject to a second review by another member of the Mandate Compliance monitoring team. Both the first and second review of new alerts are recorded within Aladdin.	<p>Inspection</p> <p>For a sample of new alerts, inspected screenshots from Aladdin to confirm they were subject to a secondary review by a separate senior team member of the Mandate Compliance monitoring team.</p> <p>Exceptions noted.</p> <p>Management self-identified 3 instances during the period where the 4-eyes review of new alerts for the day (had not been performed.</p> <p>Details of missed 4 eyes reviews (exceptions in control 18.7) and the end of day check which failed to identify the issue (exceptions in control 18.6):</p> <p>i) 1 new alert on 26 Jan 23</p> <p>ii) 1 new alert on 20 Mar 23</p> <p>ii) 1 new alert on 24 May 23</p>
18.8	On a quarterly basis, a review will be completed by a senior member of the Mandate Compliance team to confirm no compliance rules have been mistakenly removed from Portfolios by members of the EMEA Mandate Compliance Coding team. The review utilises a report of removed rules provided by BRS. Any issues identified by the review process will be investigated and followed up with the coding analyst if required. Where a rule is identified as having been mistakenly removed, the rule will be reinstated immediately, and a retrospective check performed for the period when the rule was not operating.	<p>Inspection</p> <p>For a sample of quarters, inspected the annotated BRS report and email proof of review to confirm a senior member of the Mandate Compliance team reviewed and investigated any issues as required. For the sample of quarters tested no rules were identified as having been mistakenly removed.</p> <p>No exceptions were identified.</p>

The mandate compliance team provides independent oversight of trading and examine any breaches that arise. They investigate potential breaches of investment guidelines, which are identified post trade. Post trade breaches are monitored daily, and investigated to determine how the violation has occurred, and whether any rule overrides were applied by the fund manager. Potential breaches are escalated and where it is established that an actual breach has occurred this will be recorded in the Mandate Compliance breach log. Columbia Threadneedle Investments EMEA input active breaches into the global risk management system, MetricStream.

The risk management system is also used to capture all risk events, where there has been a potential or actual impact, including when a client has been financially disadvantaged and reimbursement or compensation has been paid. All risk events are subject to independent review by Operational Risk prior to closure, with management information in relation to trends in risk events and individual material errors reported to the EMEA RCC.

19	Controls provide reasonable assurance that transaction errors (including guideline breaches, trading errors and client reporting errors) are identified, reported to clients and resolved in accordance with established policies.	
	Control Procedure	PwC Testing Procedures and Results
19.1	Where a REV is raised as an active breach for a mandate breach or trade error for transactional errors, it is independently reviewed by Operational Risk prior to closure to ensure that remedial action is taken to close it. This includes any client reimbursements required.	<p>Inspection For a sample of REV's impacting in scope portfolios, inspected the REV report to confirm it was prepared, remedial action was taken, and final reviewed by Operational Risk prior to closure.</p> <p>No exceptions were identified.</p> <p>Inspection For a sample of client reimbursements, inspected the REV reports to confirm that client reimbursement details were recorded.</p> <p>No exceptions were identified.</p>
19.2	Management information regarding REV's and individual significant errors are reported to the firm's regional Risk & Controls Committee (EMEA RCC) on a monthly basis. High-level trend analysis and aged open Risk Event action monitoring forms part of the management information submitted to the EMEA RCC. Minutes of these meetings are produced and approved.	<p>Inspection For a sample of months, inspected the approved minutes from the meeting of the EMEA Risk & Controls Committee to confirm that management information regarding REV's and significant errors were reported, including high level trend analysis and ageing of open Risk Event actions.</p> <p>No exceptions were identified.</p>
19.3	For all trade errors, mandate (guideline) breaches and external (client) reporting errors recorded as risk events (REV's) on MetricStream (MS) as having client impact, ORM will check that evidence of client notification, when required, has been obtained and attached in MS by the respective Risk Liaison Officer (RLO). Any exceptions will be investigated and resolved by ORM prior to closure of the REV.	<p>Inspection For a sample of trade errors, mandate (guideline) breaches and external (client) reporting errors recording as risk events (REV's) on MetricStream (MS) as having client impact, inspect proof that the ORM checked the confirmation from Client services and that it was completed in MS by the Risk Liaison Officer (RLO). Inspect proof that any exceptions have been investigated and resolved by ORM prior to closure of REV.</p> <p>No exceptions were identified.</p>

There are three potential sources of counterparty exposure for Columbia Threadneedle's institutional clients through their segregated accounts:

1: Tier 1 FX/Derivatives:

OTC derivatives can only be dealt with approved counterparties (Tier 1 FX and Derivative brokers). An open derivative position could lead to a counterparty risk exposure, but all derivative positions are fully collateralised with cash to a pre-defined threshold.

2: Tier 2 Cash Bond and Cash Equity brokers:

Equities and fixed income securities. For this class of counterparty there is no exposure – all dealing is done on a delivery vs. payment (DVP) basis. Broker approval controls provide management assurance that all counterparties used for execution are on the approved list.

3: Tier 3 Cash Issuers:

Cash deposits only and money market instruments. All deposit takers must be approved and reviewed on a regular basis.

20	Controls provide reasonable assurance that counterparty exposures are monitored for compliance with the firm's limits and guidelines.	
	Control Procedure	PwC Testing Procedures and Results
20.1	New FX/Derivative counterparties (T1) counterparties are approved by two members of the Counterparty Credit Risk Committee after due diligence of the new counterparty has been performed. On confirmation of approval from the Counterparty Credit Risk Committee, email notification is sent to both legal and the CTI Operations Team requesting for documentation set-up with the T1 Counterparty and internal set-up of the counterparty on Aladdin post legal documents in place.	Reliance on Risk and Control Services team Inspection For a sample of new FX/Derivative (T1) counterparty requests, inspected the approved Counterparty Risk Credit Risk Committee minutes and due diligence forms for evidence that due diligence was completed and the brokers were approved by the Counterparty Credit Risk Manager and two other members of the Counterparty Credit Risk Committee before being added to Aladdin. No exceptions were identified.
20.2	New cash bond/cash equity (T2) and new money market instrument (T3) counterparties are approved by two members of the Counterparty Credit Risk Committee after due diligence of the new counterparty has been performed. On confirmation of approval from the Counterparty Credit Risk Committee, email notification is sent to the Columbia Threadneedle Operations Team requesting set-up of the T2/T3 counterparty on Aladdin.	Reliance on Risk and Control Services team Inspection For a sample of new cash bond/cash equity (T2) & new money market instrument (T3) counterparty requests, inspected the approved Counterparty Credit Risk Committee minutes and due diligence forms to confirm that due diligence have been completed and the brokers have been approved appropriately by the Counterparty Credit Risk Manager and two other members of the Counterparty Credit Risk Committee before being added to Aladdin. No exceptions were identified.
20.3	On an annual basis, a full reconciliation is completed between Approved Counterparty/Broker lists and the trading systems (T1, T2, T3 brokers). Any exceptions are investigated and resolved.	Inspection Inspected evidence to confirm that a reconciliation between the Approved Counterparty/Broker List and the trading systems (T1, T2, T3 brokers) is undertaken annually and any exceptions are investigated and resolved. No exceptions were identified.

20.4	Approved FX/Derivative (T1) and money market instrument (T3) counterparties are periodically reviewed within the time frames detailed within the Counterparty Credit Risk Management Policy (Appendix 4.1). All reviews are approved by two members of the Counterparty Credit Risk Committee.	<p>Inspection</p> <p>For a sample of FX/Derivative (T1) and money market instrument (T3) counterparties, inspected broker review forms and Counterparty Credit Risk Committee minutes to confirm they were reviewed in line with policy and approved by the Counterparty Credit Manager and two members of the Counterparty Credit Risk Committee.</p> <p>No exceptions were identified.</p>
20.5	System-enforced controls (e.g., broker code recognition within Aladdin) provide assurance that transactions can only be booked against counterparties, which are on the Approved Broker List.	<p>Observation</p> <p>Confirmed through observation that only authorised counterparties were able to be selected when conducting trades within the dealing system.</p> <p>No exceptions were identified.</p>
20.6	New and amendments to CSAs are set up on Aladdin by the Derivative team. There is a secondary review and approval of all new and amendments to CSAs.	<p>Inspection</p> <p>For a sample of new and amendments to CSA's during the period, inspected Aladdin screenshots to confirm they were set up by the Derivative team and there was a secondary review and approval.</p> <p>No exceptions were identified.</p>
20.7	A daily collateral process is performed managing the Client's bilateral OTC exposure versus the Counterparty in line with the terms of the CSA. Calls are delivered to the Counterparty to meet notification timelines. Any disputes aged greater than 1 day where the counterparty disputes the call amount are researched, documented and resolved to ensure Client exposure is limited to the minimum threshold/transfer amount detailed within the CSA. Any of these disputes aged greater than 5 days are documented and escalated to senior management.	<p>Reliance on Risk and Control Services team</p> <p>Inspection</p> <p>For a sample of days, inspected Aladdin system extracts and daily dispute logs to confirm that calls are delivered to meet notification timelines and any disputes are researched, documented and resolved. Any disputes longer than 5 days are documented and escalated to senior management.</p> <p>No exceptions were identified.</p>
20.8	Manual Rule Tests are set up in Aladdin where mandate restrictions cannot be automatically monitored by the system. Generated alerts are actioned by the Mandate Compliance team, in accordance with the associated manual rule test procedure at the defined interval. Identified exceptions are investigated in line with policy.	<p>Inspection</p> <p>For a sample of manual rule tests, inspected evidence that the manual rule test was actioned by a member of the Mandate Compliance Team and identified exceptions are investigated in line with policy.</p> <p>No exceptions were identified.</p>

20.9	<p>On a daily basis, a member of the Mandate Compliance Team extracts and reviews an end-of-day report from Aladdin containing all live violations and a rationale is added for any alerts which are pending action or are closed without a future test date. This review is evidenced via email sign-off.</p>	<p>Inspection</p> <p>For a sample of days, inspected evidence of the review of the end of day report from Aladdin containing all live violations and confirmed that a rationale was added for any alerts which were pending action or were closed without a future test date and an email was sent to Mandate Compliance team for proof of review.</p> <p>Exceptions noted.</p> <p>Management self-identified two instances during the period where the end of day check (Control 18.6) had not been performed:</p> <ul style="list-style-type: none"> i) End of day review for 9 Feb 23 ii) End of day review for 26 July 2023 (additional MIE communicated to PwC on 10/08/2023) <p>Inspection</p> <p>Confirmed through inspection of one end of day report from Aladdin containing all live violations of manual and automated rules triggered the previous day that the data contained within it completely and accurately reflected the data held on Aladdin.</p> <p>No exceptions were identified.</p>
20.10	<p>On a daily basis, the Mandate Compliance monitoring team are responsible for reviewing all new and repeating alerts generated by the overnight batch process in Aladdin. All new alerts generated (i.e., those alerts which have an age of 1 day) are subject to a second review by another member of the Mandate Compliance monitoring team. Both the first and second review of new alerts are recorded within Aladdin.</p>	<p>Inspection</p> <p>For a sample of new alerts, inspected screenshots from Aladdin to confirm they were subject to a secondary review by a separate senior team member of the Mandate Compliance monitoring team.</p> <p>Exceptions noted.</p> <p>Management self-identified 3 instances during the period where the 4-eyes review of new alerts for the day (had not been performed.</p> <p>Details of missed 4 eyes reviews (exceptions in control 18.7) and the end of day check which failed to identify the issue (exceptions in control 18.6):</p> <ul style="list-style-type: none"> i) 1 new alert on 26 Jan 23 ii) 1 new alert on 20 Mar 23 ii) 1 new alert on 24 May 23

20.11	On a quarterly basis, a review will be completed by a senior member of the Mandate Compliance team to confirm no compliance rules have been mistakenly removed from Portfolios by members of the EMEA Mandate Compliance Coding team. The review utilises a report of removed rules provided by BRS. Any issues identified by the review process will be investigated and followed up with the coding analyst if required. Where a rule is identified as having been mistakenly removed, the rule will be reinstated immediately, and a retrospective check performed for the period when the rule was not operating.	<p>Inspection</p> <p>For a sample quarters, inspected the review of compliance rules to confirm that it was reviewed by a senior member of the Mandate Compliance team and any issues identified are investigated and followed up. Where a rule is mistakenly removed confirm that the rule is reinstated immediately and a retrospective check performed for the period when the rule was not operating.</p> <p>No exceptions were identified.</p>
-------	---	--

Columbia Threadneedle Investments EMEA's operating model incorporates the outsourcing of a number of processes to third-party subservice organisations. A formal service management framework is in place to provide assurance that material third party service providers meet the standards required by Columbia Threadneedle Investments EMEA, as documented in contracts. These are measured through Service Level Agreements (SLAs), which contain key performance indicators (KPI) specifying the services and standards, which the third-party subservice organisations are required to achieve. Any amendments to approved Service Level Agreements will go through an internal approval and sign-off process before they can be updated. The outsourced business operations activities are overseen by dedicated oversight functions through daily monitoring of service provision, and oversight meetings are held to review management information and KPI's reflecting agreed service standards and any operational issues experienced since the previous meeting, together with the overall effectiveness of the service. Any issues identified between parties are minuted and monitored to ensure service levels are maintained.

Columbia Threadneedle Investments EMEA undertakes reviews and analyses the ISAE 3402 or equivalent reports produced for these third-party subservice organisations to assess any reported exceptions for potential impact on our control environment.

21	Controls provide reasonable assurance that outsourced activities provided by Subservice Organisations are governed by contracts and service level agreements that are authorised and subject to regular review.	
	Control Procedure	PwC Testing Procedures and Results
21.1	Signed supplier Master Agreements are in place with HSBC, Citi and BRS. Any contractual amendments to the HSBC, Citi and BRS Master Agreements requiring Director or Director-delegated authorised signatories' signatures are approved via Ariba.	<p>Inquiry</p> <p>Verify that any contractual amendments to the HSBC, Citi and BRS Master Agreements requiring Director or Director delegated authorised signatories signature were approved via Ariba.</p> <p>No exceptions were identified.</p>
21.2	On an annual basis, the Oversight Team perform a complete review of third party providers' SLAs which is subject to secondary review via email sign-off. Changes to the SLA are formally signed off via the Change Process.	<p>Reliance on Risk and Control Services team</p> <p>Inspection</p> <p>Inspected the annual review of SLAs to confirm it was subject to secondary review via email sign off.</p> <p>No exceptions were identified.</p>

21.3	On an annual basis, management undertake a review of the BRS SLAs and associated monitoring. Findings are reported to the EMEA RCC for approval of the ongoing adequacy of the SLA in effectively managing the relationship with BRS.	Reliance on Risk and Control Services team Inspection For a sample of third party service provider Internal Controls Reports, inspected the review to confirm that Management had reviewed the report at the control objective level, evaluated identified exceptions and evaluated user control considerations. No exceptions were identified.
22	Controls provide reasonable assurance the services provided by the Subservice Organisations are regularly monitored and assessed against the standards set out in the service level agreements.	
	Control Procedure	PwC Testing Procedures and Results
22.1	Annual ISAE 3402 (or equivalent) Internal Control Reports produced by HSBC and Citi are reviewed by the FA Oversight team at the control objective level, evaluating identified exceptions and user considerations. Where the third-party management response is insufficient, exceptions and qualifications in the reports are escalated to the relationship manager for resolution and/or risk acceptance.	Reliance on Risk and Control Services team Inspection For a sample of third party service provider Internal Controls Reports, inspected the review to confirm that Management had reviewed the report at the control objective level, evaluated identified exceptions and evaluated user control considerations, and that exceptions were escalated to the relationship manager for resolution where required. No exceptions were identified. Inspection Inspected CAR meeting minutes for evidence that qualifications were escalated for review and resolution. No exceptions were identified.
22.2	Monthly Service Review Meetings are held with Citi and HSBC to review key performance indicators reflecting agreed service standards and discuss operational issues and the overall effectiveness of the relationship. Key issues are minuted and reviewed for progress at the following meeting to ensure that service levels are maintained.	Reliance on Risk and Control Services team Inspection For a sample of months and quarters, inspected meeting minutes to confirm that Monthly Oversight Meetings were held with the third party service providers and that KPIs were reviewed and key issues were discussed. No exceptions were identified.

Reporting to Clients

Columbia Threadneedle Investments EMEA's Institutional clients can be provided with daily, weekly, monthly, quarterly and annual reports as well as ad-hoc reports. Investor Reporting's standard report offerings provide detailed client specific information including performance results and attribution versus the chosen benchmark, portfolio holdings and characteristics, commentary on economic conditions and market outlook. Monthly and quarterly reports are generally provided within 20 business days of the month/quarter end. Investor Reporting also offers clients a comprehensive financial statement package, which include information regarding Portfolio Holdings, Portfolio Transactions, Income and Valuations.

The scope of this controls report only includes the controls designed to ensure the completeness and accuracy of portfolio holdings, portfolio transactions, income and valuation data distributed by the Investor Reporting team. Additionally, bespoke valuation reports distributed by our Pricing team and bespoke transaction reports distributed by our Client Services team are also included in the scope of this report. Other data may be provided to clients, but this is not covered in the scope of this report.

Client's reporting requirements, including report content, frequency and delivery deadlines will be determined during the on-boarding process and agreed through inclusion within the IMA. A reporting timetable is maintained that ensures all reports are produced and delivered to the timeline agreed with clients. Following production and prior to despatch all reports are subject to internal quality assurance by the Investor Reporting team and where specifically requested, the client service team and the portfolio manager. Subsequent requests or changes to requirements, post on-boarding, are reviewed and managed via an internal change process with the same controls and protocols to ensure timetables and associated documentation are updated in a timely manner.

23	Controls provide reasonable assurance that client reporting in respect of portfolio valuation, transactions, holdings and income is complete and accurate and provided within agreed timescales.	
	Control Procedure	PwC Testing Procedures and Results
23.1	From 1 October 2022 to 31 July 2023, all statements (reports, from 1 August 2023 onwards) are independently reviewed and approved by authorized members of the Client Reporting Team. A report completion checklist is used to review all client investment reports, automated client financial statements and send-on reports for completeness and accuracy. The checklist is subject to a secondary independent review prior to release.	Inspection For a sample of in-scope client statements (reports from 01 August 2023 onwards), inspected evidence that they are authorised by members of the Client Reporting Team. Further, inspected the report completion checklist along with evidence of secondary review prior to release. No exceptions were identified.
23.2	An authorised member of the Client Reporting Team monitors sign-off of the monthly report generation process to ensure all client statements have been produced for the period, required reviews have been completed and reports are sent to the clients timely.	Inspection For a sample of months, inspected the management information timetable to confirm that client specified deadlines were monitored for in-scope client reporting. No exceptions were identified. Inspection For a sample of months, inspected Manager Sign off checklist for evidence of review and sign off to confirm that all required in-scope client statements have been completed and sent to the clients within the specified timelines. No exceptions were identified.
23.3	Bespoke client reports generated are reviewed to ensure completeness and accuracy and signed off prior to being released for onward distribution. The review is evidenced either via e-mail or an electronic checklist.	Inspection For a sample of in-scope bespoke client reports, inspected email correspondence and checklists to confirm that client reports were reviewed and signed off prior to release. No exceptions were identified.

23.4	<p>October 1, 2022 – April 30, 2023</p> <p>Monthly, a series of data quality checks is performed by Information Management over data transferred from the portfolio management system to client reporting systems. Discrepancies are researched and resolved. Client Reporting is notified after discrepancies have been resolved.</p> <p>May 1, 2023 – September 30, 2023</p> <p>Monthly, a series of data quality checks is performed by Information Management over data transferred from the portfolio management system to client reporting systems. Discrepancies are researched and resolved. Client Reporting is notified after discrepancies have been resolved. Failed data quality checks are monitored daily for completeness of research and resolution.</p>	<p>October 1, 2022 – April 30, 2023</p> <p>Inspection</p> <p>For a sample of months, inspected quality checks were performed by Information Management for data transfers between portfolio management systems and client reporting systems. Further validated that discrepancies are researched and resolved.</p> <p>Exceptions noted.</p> <p>Management self-identified that 3 out of a population of 422 failed data quality checks were not adequately researched and resolved.</p> <p>No additional exceptions noted from PwC testing.</p> <p>May 1, 2023 – September 30, 2023</p> <p>Inspection</p> <p>For a sample of months, inspected quality checks were performed by Information Management for data transfers between portfolio management systems and client reporting systems, to determine whether discrepancies were researched and resolved.</p> <p>No exceptions were identified.</p> <p>Inspection</p> <p>For a sample of quality checks, inspected management's daily monitoring to determine whether it was performed for completeness of research and resolution of failed data quality checks.</p> <p>No exceptions were identified.</p> <p>Reperformance</p> <p>For a sample of failed quality checks, reperfomed management's daily monitoring to determine whether a failure alert was sent for each failed quality check and that the daily quality check monitoring was performed to match the failure with an incident ticket and email alert.</p> <p>No exceptions were identified.</p>
------	---	---

Restricting Access to Systems and Data

Columbia Threadneedle Investments EMEA commits considerable resources, both human and technological, to provide clients with the best quality of service. Maintaining the integrity of the Technology infrastructure is taken very seriously. Our server environments in the London (Global Switch & Equinix) and St. Louis (Kyndryl) data centres are provided by a specialised third party, who

offer fully resilient and secure facilities. There are defined processes to monitor effectiveness of the third party in managing our data centres through periodic service review meetings and review of their annual assurance reports, which cover key areas including physical access and environmental safeguards. Physical access to these data centres is subject to strict controls and Technology management undertake regular reviews to ensure that access has only been granted to approved users in accordance with names provided to the third party as authorised by Columbia Threadneedle Investments EMEA.

24	Physical access to in-scope systems is restricted to authorized individuals	
	Control Procedure	PwC Testing Procedures and Results
24.1	On an annual basis, reviews are performed over third-party service providers ISAE 3402 (or equivalent) internal Control Reports at the control objective level and user considerations are evaluated.	Inspection For a sample of third-party service providers inspected the results of management's review of ISAE 3402 (or equivalent) internal Control Reports to confirm that it was performed, and user considerations were evaluated. No exceptions were identified.
24.2	Access to secure data center facilities is reviewed and approved at least quarterly based on job responsibilities.	Inspection For a sample of quarterly reviews, inspected the results of management's review to confirm that access to the data centre was reviewed and approved. No exceptions were identified.

Systems have been configured with passwords to secure programs, data and information resources. Parameters are enforced in line with our internal Access Control Standard and require a combination of length, expiration, complexity, history, account lock-out and idle session time-out settings. Where we use third party applications, some will have their own policies and standards that may differ from ours. Where there is a difference in password policies, we perform a review and document the risk to ensure mitigating controls are identified and any residual risks are understood and accepted by management.

Logical access to programs, data and information resources requires approval by one of the following: the requestor's leader, the environment owner or the environment owner's delegate. Each member of staff is provided with a unique user ID and password, which gives restricted access based on permission protocols. HR provide Technology with notification of staff leaving the organisation, and this enables access to the network, and any application specific access to be removed in a timely manner. On a monthly basis the Technology Risk team carry out a review of all users who have left the organisation in the preceding month, to make sure that their access rights have been removed. Any exceptions are followed up to make sure access is removed and that the application(s) has not been accessed after the user's last day in the office.

Segregation of access exists between Technology Operations staff, development staff, and the business user community. Privileged Technology access, including the ability to create, modify and remove user access, is restricted to authorised individuals based on job responsibility, which is segregated from business operational responsibilities. All user access, including privileged access is reviewed on a quarterly basis. Access is granted to individual users, and any instance where it is necessary to share an account and assign more than one user is subject to appropriate management review and approval, leveraging the Password Management Tool.

25	Controls provide reasonable assurance that logical access to In-scope systems and data is restricted to authorised individuals in accordance with job roles and/or business requirements and that client and third-party access to In-scope systems and data is restricted and/or monitored.								
	<table border="1"> <thead> <tr> <th data-bbox="308 275 1066 342">Control Procedure</th><th data-bbox="1074 275 1428 342">PwC Testing Procedures and Results</th></tr> </thead> <tbody> <tr> <td data-bbox="228 353 1066 689"> 25.1 Prior to access being granted by authorised system administrators, requests for new or modified systems access accounts are approved by at least one of the following: the requestor's leader, the Environment Owner, or the Environment Owner's delegate. </td><td data-bbox="1074 353 1428 689"> Inspection For a sample of management's semi-annual review, inspected the results of management's review to confirm that new or modified access requests to in-scope applications were approved prior to the access being granted by authorised system administrators. No exceptions were identified. </td></tr> <tr> <td data-bbox="228 701 1066 1126"> 25.2 Management reviews that the password parameters for in-scope systems and applications are in line with the Password Controls Standard at least annually. Any deviation from the firm's Password Controls Standard requires approval by the Head of IT. (Note: FactSet is authenticated via individual's FactSet.net ID and 2FA passcode delivered to their corporate email address upon creation of new account. There is no user created password for the installed application.) </td><td data-bbox="1074 701 1428 1126"> Inspection For a sample of systems and applications, inspected the results of management's review of password parameters to confirm that management had reviewed the password parameters for critical systems and applications in scope at least annually and that any deviations from the Password Controls Standard were approved by the Head of IT. No exceptions were identified. </td></tr> <tr> <td data-bbox="228 1137 1066 1684"> 25.3 For UK-managed applications, on a monthly basis, an oversight report of leaver accounts is reviewed to identify any instance where logical access has not been removed, exceptions identified are remediated in a timely manner. For US-managed applications, Network access (Single Sign-On and Active Directory) is automatically removed upon user termination. </td><td data-bbox="1074 1137 1428 1684"> Inspection Inspected a sample of the monthly oversight report of leavers accounts to confirm that management had reviewed the report to identify that access for leavers had been removed from the network, critical applications and supporting infrastructure and that any exceptions identified were remediated timely. For US managed applications, inspected evidence to determine whether network access (Single Sign-On and Active Directory) is automatically removed upon user termination. </td></tr> </tbody> </table>	Control Procedure	PwC Testing Procedures and Results	25.1 Prior to access being granted by authorised system administrators, requests for new or modified systems access accounts are approved by at least one of the following: the requestor's leader, the Environment Owner, or the Environment Owner's delegate.	Inspection For a sample of management's semi-annual review, inspected the results of management's review to confirm that new or modified access requests to in-scope applications were approved prior to the access being granted by authorised system administrators. No exceptions were identified.	25.2 Management reviews that the password parameters for in-scope systems and applications are in line with the Password Controls Standard at least annually. Any deviation from the firm's Password Controls Standard requires approval by the Head of IT. (Note: FactSet is authenticated via individual's FactSet.net ID and 2FA passcode delivered to their corporate email address upon creation of new account. There is no user created password for the installed application.)	Inspection For a sample of systems and applications, inspected the results of management's review of password parameters to confirm that management had reviewed the password parameters for critical systems and applications in scope at least annually and that any deviations from the Password Controls Standard were approved by the Head of IT. No exceptions were identified.	25.3 For UK-managed applications, on a monthly basis, an oversight report of leaver accounts is reviewed to identify any instance where logical access has not been removed, exceptions identified are remediated in a timely manner. For US-managed applications, Network access (Single Sign-On and Active Directory) is automatically removed upon user termination.	Inspection Inspected a sample of the monthly oversight report of leavers accounts to confirm that management had reviewed the report to identify that access for leavers had been removed from the network, critical applications and supporting infrastructure and that any exceptions identified were remediated timely. For US managed applications, inspected evidence to determine whether network access (Single Sign-On and Active Directory) is automatically removed upon user termination.
Control Procedure	PwC Testing Procedures and Results								
25.1 Prior to access being granted by authorised system administrators, requests for new or modified systems access accounts are approved by at least one of the following: the requestor's leader, the Environment Owner, or the Environment Owner's delegate.	Inspection For a sample of management's semi-annual review, inspected the results of management's review to confirm that new or modified access requests to in-scope applications were approved prior to the access being granted by authorised system administrators. No exceptions were identified.								
25.2 Management reviews that the password parameters for in-scope systems and applications are in line with the Password Controls Standard at least annually. Any deviation from the firm's Password Controls Standard requires approval by the Head of IT. (Note: FactSet is authenticated via individual's FactSet.net ID and 2FA passcode delivered to their corporate email address upon creation of new account. There is no user created password for the installed application.)	Inspection For a sample of systems and applications, inspected the results of management's review of password parameters to confirm that management had reviewed the password parameters for critical systems and applications in scope at least annually and that any deviations from the Password Controls Standard were approved by the Head of IT. No exceptions were identified.								
25.3 For UK-managed applications, on a monthly basis, an oversight report of leaver accounts is reviewed to identify any instance where logical access has not been removed, exceptions identified are remediated in a timely manner. For US-managed applications, Network access (Single Sign-On and Active Directory) is automatically removed upon user termination.	Inspection Inspected a sample of the monthly oversight report of leavers accounts to confirm that management had reviewed the report to identify that access for leavers had been removed from the network, critical applications and supporting infrastructure and that any exceptions identified were remediated timely. For US managed applications, inspected evidence to determine whether network access (Single Sign-On and Active Directory) is automatically removed upon user termination.								

25.4	Semi-annually (or quarterly for privileged access to SOX, SOC2, ISAE3402, and Ameriprise Bank FSB assets), Environment Owners or delegates review access to determine if access rights are appropriate for the user's job responsibilities. Requests to revoke or modify access are submitted when access is deemed inappropriate.	<p>Inspection</p> <p>For a sample of quarters and applications inspected the access recertification review results for in-scope system environments, applications and databases, to confirm that access had been reviewed and approved by environment owners based on job responsibilities.</p> <p>No exceptions were identified.</p> <p>Inspection</p> <p>Inspected accounts' revocation requests from the recertification review and database access profiles review, to confirm that access had been revoked per the environment owner's request.</p> <p>No exceptions were identified.</p>
25.5	Quarterly, the Identity and Access Governance team reviews the PAM Inventory Report to confirm faceless IDs in Aveksa are in the Privileged Account Management (PAM) system. Faceless IDs not in the PAM system are managed to resolution.	<p>Inspection</p> <p>For a sample of quarterly PAM inventory report reviews, inspected the results of the review to confirm that the report is reviewed by the Identity and Access Governance team and inappropriate Faceless IDs are managed to resolution.</p> <p>No exceptions were identified.</p>

Functionality within critical applications is defined and allocated to ensure sufficient segregation of duties exists, and system owners review the pre-defined segregation of duties matrices annually to ensure they remain current. In the order management systems Aladdin and Commodities DST, there is system-enforced segregation of duties between people approved to authorise and execute investment transactions. This is required as these applications are market facing and cover critical trading activities.

26	Controls provide reasonable assurance that segregation of incompatible duties within and across business and technology functions is formally defined, implemented, updated and enforced by logical security controls	
	Control Procedure	PwC Testing Procedures and Results
26.1	On an annual basis, the pre-defined segregation of duties matrices are reviewed by business owners, to ensure they are up to date.	<p>Inspection</p> <p>Inspected the results of business owners' reviews of pre-defined segregation of duties matrices, to confirm that they had been reviewed by the Business Owner on an annual basis.</p> <p>No exceptions were identified.</p>

26.2	There is a system-enforced segregation of duties between persons approved to authorise and execute investment transactions in Aladdin, GoldenSource and Commodities DST.	Inspection Inspected the application access to Aladdin, GoldenSource, and Commodities DST applications, to confirm that the applications were configured to enforce segregation of duties between persons approved to authorise and execute investment transactions. No exceptions were identified.
26.3	On a quarterly basis, management monitors access to the production environment via the identity access management system (Aveksa) to confirm that developers are not granted update access to the production environment and any identified SOD conflicts were investigated and resolved in a timely manner.	Inspection For a sample of quarters, inspected the results of management's review to confirm that code developers were not permitted update access to production system environments, applications and databases and migration of the approved application programs and database changes were performed by production control staff who are separate to the code development team. No exceptions noted.

Maintaining Systems Integrity

Columbia Threadneedle Investments EMEA uses batch scheduling software to ensure that programs are executed in the proper order according to defined schedules. The batch scheduling processes are tracked in logs which are monitored to ensure that errors during processing are identified, reviewed and resolved in a timely manner. There are two systems used: these are Tidal and Abinitio; both are internally hosted. The batch failure process is managed in-house and any critical batch job failure on either Tidal or Abinitio is automatically logged as an incident ticket on the Service Management System ServiceNow. The ability to modify the production system batch schedules is restricted to authorised individuals, and management performs a semi-annual review of users, with access to modify the batch scheduling tools, to ensure that access granted to users continues in line with current job responsibilities. Any changes to the batch schedules are managed through standard change management processes, and a formal change request will be raised, which will require approval before changes can be implemented into the production environment.

27	Controls provide reasonable assurance that scheduling and internal processing of data is complete, accurate and within agreed timescales.	
	Control Procedure	PwC Testing Procedures and Results
27.1	For batch job processing failures, an Incident Ticket or Alert Notification is created and sent to the appropriate team. Tickets or alerts are assigned to the appropriate Technology team and managed to resolution through the appropriate Service Management Process (Incident or Event Management).	Inspection For a sample of quarters, inspected the results of management's review to confirm that for job processing failures, tickets or alert notifications were created and assigned to the appropriate Technology team and were managed to resolution through the appropriate Service Management Process. No exceptions were identified.

27.2	<p>On a daily basis for internally managed funds, the Operations team reconciles the following transactions to Custodian data:</p> <ul style="list-style-type: none"> ■ All settled securities transactions ■ All settled cash transactions <p>Any discrepancies identified are investigated and resolved in line with policy.</p>	<p>Inspection</p> <p>For a sample of days, inspected completed cash and asset reconciliations to confirm that settled securities transactions and settled cash transactions were reconciled to custodian data and that any discrepancies were researched and resolved.</p> <p>No exceptions were identified.</p> <p>Reperformance</p> <p>For one cash reconciliation report, reperfomed the reconciliation using Aladdin Accounting and custodian data to confirm that the system properly identified trade activity not established and maintained timely, accurately and completely.</p> <p>No exceptions were identified.</p> <p>Reperformance</p> <p>For one asset reconciliation report, reperfomed the reconciliation using Aladdin Accounting and custodian data to confirm that the system properly identified trade activity not established and maintained timely, accurately and completely.</p> <p>No exceptions were identified.</p>
------	--	--

Systems are configured such that external communications involving client data are transmitted securely using encryption and secure server settings, through SFTP (Secure File Transfer Protocol). Cash and portfolio positions are reconciled as part of business processes on a daily basis using data received from Custodians and other third parties, and any discrepancies are researched and followed up.

28	Controls provide reasonable assurance that transmission of data to/from external parties is complete, accurate, executed within agreed timescales and secure in line with external party agreements.	
	Control Procedure	PwC Testing Procedures and Results
28.1	<p>For batch job processing failures, an Incident Ticket or Alert Notification is created and sent to the appropriate team. Tickets or alerts are assigned to the appropriate Technology team and managed to resolution through the appropriate Service Management Process (Incident or Event Management).</p>	<p>Inspection</p> <p>For a sample of quarters, inspected the results of management's review to confirm that for job processing failures, tickets or alert notifications were created and assigned to the appropriate Technology team and were managed to resolution through the appropriate Service Management Process.</p> <p>No exceptions were identified.</p>

28.2	<p>Quarterly, for the North America region, Data Management runs extracts/ reports of file transfers that includes information on the level of encryption, identifies any unencrypted file transfer protocols, and has the CDO teams confirm the level of data being transferred or the existence of an approved Standard Exception. Discrepancies identified are managed to closure through the Security Incident Management process by enabling encryption or providing an approved Standard Exception. Alternatively, the EMEA region only uses encryption and secure server settings for file transfers externally, unless there is an approved Standard Exception.</p>	<p>Inspection</p> <p>Confirmed through inspection, that external file transfers happen via a secured network for the EMEA region.</p> <p>No exceptions were identified.</p> <p>Inspection</p> <p>Inspected evidence of the encryption and secure-server settings.</p> <p>No exceptions were identified.</p>
28.3	<p>On a daily basis for internally managed funds, the Operations team reconciles the following transactions to Custodian data:</p> <ul style="list-style-type: none"> ■ All settled securities transactions ■ All settled cash transactions <p>Any discrepancies identified are investigated and resolved in line with policy.</p>	<p>Inspection</p> <p>For a sample of days, inspected completed cash and asset reconciliations to confirm that settled securities transactions and settled cash transactions were reconciled to custodian data and that any discrepancies were researched and resolved.</p> <p>No exceptions were identified.</p> <p>Reperformance</p> <p>For one cash reconciliation report, reperfomed the reconciliation using Aladdin Accounting and custodian data to confirm that the system properly identified trade activity not established and maintained timely, accurately and completely.</p> <p>No exceptions were identified.</p> <p>Reperformance</p> <p>For one asset reconciliation report, reperfomed the reconciliation using Aladdin Accounting and custodian data to confirm that the system properly identified trade activity not established and maintained timely, accurately and completely.</p> <p>No exceptions were identified.</p>

Annually, Technology operations reviews firewall placement to validate external points of connectivity to Columbia Threadneedle networks are managed, segregated into zones (for internal networks), and protected through Columbia Threadneedle firewalls. Discrepancies identified are resolved by Network Services via a ServiceNow ticket.

Columbia Threadneedle Investments EMEA manages its IT framework to mitigate against cyber threats. There are dedicated controls to ensure a robust IT framework as well as to counter malicious electronic attacks. Annually, Security Client Engineering review anti-malware configurations with Cyber Security, who provide signoff of existing agent policies for malware protection, network integrity, exploit protection, intrusion protection, device control, deny list (bans), and system. Any discrepancies identified from the review are logged in the Service Management system and remediated through the change management process.

29	Controls provide reasonable assurance that network perimeter security devices are installed, and changes are tested and approved.	
	Control Procedure	PwC Testing Procedures and Results
29.1	Semi-annually, Technology Operations reviews firewall placement to validate external points of connectivity to Ameriprise Financial networks are managed and protected through Ameriprise controlled firewalls. Discrepancies identified are resolved by Network Services via a ServiceNow ticket.	Inspection Inspected a sample of the semi-annual results of the firewall placement reviews to ensure that external points of connectivity to Ameriprise Financial networks are managed, segregated into privileged zones, and protected through Ameriprise controlled firewalls. No exceptions were identified.
29.2	Before emergency changes are implemented to production, the Group Approver or their delegate(s) provide Emergency Request for Change (ERFC) approval in the related incident ticket, or the change record.	Inspection For a sample of emergency changes, inspected respective Request for Change to confirm that it was approved by the Group Approver or their delegate(s) before change was implemented into production. No exceptions were identified.
29.3	Before changes are implemented to production, Federated Change Management teams approves the Request for Change (RFC) ticket. A script is run daily to identify changes that are not "Approved" prior to the Planned Start Date/Time and moves the RFC back to the "New" state where the changes can be rescheduled and requested for approval.	Inspection For a sample of changes, inspected the respective Request for Change to confirm that it was approved by Federated Change Management before the change was implemented into production. No exceptions were identified.
29.4	Monthly, the Change Management team reviews a sample of changes to production systems to confirm appropriate testing was performed before moving the change into production. Teams that failed to attach changes testing results to the change ticket are educated on the appropriate process.	Inspection For a sample of monthly change test reviews, inspected the results of the review to confirm that the appropriate testing was performed before moving the change into production. No exceptions were identified.

30	Controls provide reasonable assurance that anti-virus definitions are periodically updated across all terminals and servers, deployment and settings are periodically reviewed and updated when required; and patterns of attempted external breaches are monitored	
	Control Procedure	PwC Testing Procedures and Results
30.1	Monthly, Security Client Engineering confirms anti-malware signature levels are current on Microsoft Windows servers and workstations. Anti-Malware signatures that are not updated within the established timeframe are managed to resolution through the Service Now Problem Management or Incident Management process.	Inspection For a sample of months inspected results of Information Security Services (ISS) reviews of Microsoft Windows servers and endpoints anti-malware signatures to confirm that this is reviewed by Security Client Engineering and any findings are managed to resolution through Service Now Problem/Incident management process. No exceptions were identified.
30.2	Daily, Information Security Services (ISS) reviews information security threats identified from external sources. Threats are monitored and reported to the TELM.	Inspection For a sample of days inspected the results of Information Security Services (ISS) reviews of security threats identified from threat sources to ensure that they have been actioned as needed. No exceptions were identified.
30.3	Security Client Engineering reviews anti-malware configurations, for all supported servers and endpoints, with Cyber Security on an annual basis to confirm settings are configured appropriately. Any discrepancies identified as part of the review would be subsequently remediated within the change management process.	Inspection Inspected the results of Security Client Engineering's reviews on anti malware configurations to confirm settings were configured appropriately and any discrepancies identified were subsequently remediated within the change management process. No exceptions were identified.
31	Controls provide reasonable assurance that data received from external parties is scanned for known vulnerabilities, any compromised data is quarantined, and definitions of threats are periodically updated	
	Control Procedure	PwC Testing Procedures and Results
31.1	Monthly, Security Client Engineering confirms anti-malware signature levels are current on Microsoft Windows servers and workstations. Anti-Malware signatures that are not updated within the established timeframe are managed to resolution through the Service Now Problem Management or Incident Management process.	Inspection For a sample of months inspected the results of Information Security Services (ISS) reviews of Microsoft Windows servers and endpoints anti-malware signatures to confirm that this is reviewed by Security Client Engineering and any findings are managed to resolution through Service Now Problem/Incident management process. No exceptions were identified.

31.2	Daily, Information Security Services (ISS) reviews information security threats identified from external sources. Threats are monitored and reported to the TELM.	Inspection For a sample of days inspected the results of Information Security Services (ISS) reviews of security threats identified from threat sources to ensure that they have been actioned as needed. No exceptions were identified.
31.3	Security Client Engineering reviews anti-malware configurations, for all supported servers and endpoints, with Cyber Security on an annual basis to confirm settings are configured appropriately. Any discrepancies identified as part of the review would be subsequently remediated within the change management process.	Inspection Inspected the results of Security Client Engineering's reviews on anti-malware configurations to confirm settings were configured appropriately and any discrepancies identified were subsequently remediated within the change management process. No exceptions were identified.

Maintaining and Developing Systems Hardware and Software

Changes to infrastructure, network, software and supporting systems follow a consistent process and controls Governed by defined policies and standards, management undertake periodic reviews of all changes to production systems to check that they have been implemented in accordance with these controls. For internally developed applications, this includes the use of version control software, which makes sure that the correct version of the application program is being changed and that the correct versions of the application programmes are released into the production environment following completion of testing and approval.

Change requests are documented in a Service Management System, which includes a detailed description of the change, requestor information and categorisation based on the scale and type of change. Changes are developed by code developers who are not permitted update access to the production system environments, applications and databases. Prior to implementation into the production environments changes are appropriately tested and authorised following defined policies and standards.

For any change that involves the migration of data between systems, policies and procedures require that the impacted data is tested via technical and business reconciliations, between the source and destination system. This is to ensure that no significant data discrepancies are left unresolved prior to implementation into the new system.

Logically separate development, test and production environments are maintained for all in-scope applications and access is restricted to authorised individuals. Only Technology Operations staff are permitted access to production system environments, applications and databases.

32	Controls provide reasonable assurance that development and implementation of both in house and third-party in-scope systems are authorised, tested and approved	
	Control Procedure	PwC Testing Procedures and Results
32.1	Before emergency changes are implemented to production, the Group Approver or their delegate(s) provide Emergency Request for Change (ERFC) approval in the related incident ticket, or the change record.	Inspection For a sample of emergency changes, inspected the respective Request for Change to confirm that it was approved by the Group Approver or their delegate(s) before the change was implemented into production. No exceptions were identified.
32.2	Before changes are implemented to production, Federated Change Management teams approves the Request for Change (RFC) ticket. A script is run daily to identify changes that are not "Approved" prior to the Planned Start Date/Time and moves the RFC back to the "New" state where the changes can be rescheduled and requested for approval.	Inspection For a sample of changes, inspected the respective Request for Change to confirm that it was approved by Federated Change Management before change was implemented into production. No exceptions were identified.
32.3	Monthly, the Change Management team reviews a sample of changes to production systems to confirm appropriate testing was performed before moving the change into production. Teams that failed to attach changes testing results to the change ticket are educated on the appropriate process.	Inspection For a sample of monthly change test reviews, inspected the results of the review to confirm that the appropriate testing was performed before moving change into production. No exceptions were identified.
32.4	On a quarterly basis, management monitors access to the production environment via the identity access management system (Avekso) to confirm that developers are not granted update access to the production environment and any identified SOD conflicts were investigated and resolved in a timely manner.	Inspection For a sample of quarters, Inspected the results of management's review to confirm that code developers were not permitted update access to production system environments, applications and databases and migration of the approved application programs and database changes were performed by production control staff who are separate to the code development team. No exceptions were identified.
32.5	Logically separate development, testing, and production environments have been established and are restricted to authorised individuals.	Inspection For a sample of applications, inspected evidence that the development, testing and production environments were logically separated and restricted to authorised individuals. No exceptions were identified.

32.6	For self-maintained applications, Version Control Software is in place to ensure that the correct version of the application program is being changed and the correct version of the application programs are being released to the production environment upon testing and approval.	Observation For self-maintained applications, observed that version control software was in place to confirm that the correct version of the application program was being changed upon approval of a change request and that the correct version of the application programs were released to the production environment upon testing and approval. No exceptions were identified.
32.7	On an annual basis, reviews are performed over third-party service providers ISAE 3402 (or equivalent) Internal Control Reports at the control objective level and user considerations are evaluated.	Inspection For a sample of third-party service providers inspected the results of management's review of ISAE 3402 (or equivalent) internal Control Reports to confirm that it was performed, and user considerations were evaluated. No exceptions were identified.
33	Controls provide reasonable assurance that data migration or modification is authorised, tested and, once performed, reconciled back to the source data	
	Control Procedure	PwC Testing Procedures and Results
33.1	Where required data conversion is tested via technical and business reconciliations between source and destination systems and approved prior to implementation in the production environment. Any identified exceptions are prioritised and monitored to satisfactory resolution through appropriate governance.	Inquiry Inquired of management to confirm that there were no relevant data migrations within the period. Therefore, the operating effectiveness of this control activity could not be tested. No exceptions noted.
33.2	New systems/enhancements are adequately tested and approved before being migrated into production.	Inspection For the Hiport to Aladdin cut-over, inspected that management performed user acceptance testing for the change. No exceptions were identified.
34	Controls provide reasonable assurance that changes to existing in-scope systems, including hardware upgrades, software patches and direct configuration changes, are authorised, tested and approved in line with policy	
	Control Procedure	PwC Testing Procedures and Results
34.1	Before emergency changes are implemented to production, the Group Approver or their delegate(s) provide Emergency Request for Change (ERFC) approval in the related incident ticket, security incident ticket, or the change record.	Inspection For a sample of emergency changes, inspected the respective Request for Change to confirm that it was approved by the Group Approver or their delegate(s) before the change was implemented into production. No exceptions were identified.

34.2	Before changes are implemented to production, Federated Change Management teams approves the Request for Change (RFC) ticket. A script is run daily to identify changes that are not "Approved" prior to the Planned Start Date/Time and moves the RFC back to the "New" state where the changes can be rescheduled and requested for approval.	<p>Inspection</p> <p>For a sample of changes, inspected the respective Request for Change to confirm that it was approved by Federated Change Management before change was implemented into production.</p> <p>No exceptions were identified.</p>
34.3	Monthly, the Change Management team reviews a sample of changes to production systems to confirm appropriate testing was performed before moving the change into production. Teams that failed to attach changes testing results to the change ticket are educated on the appropriate process.	<p>Inspection</p> <p>For a sample of monthly change test reviews, inspected the results of the review to confirm that the appropriate testing was performed before moving change into production.</p> <p>No exceptions were identified.</p>
34.4	On a quarterly basis, management monitors access to the production environment via the identity access management system (Aveksa) to confirm that developers are not granted update access to the production environment and any identified SOD conflicts were investigated and resolved in a timely manner.	<p>Inspection</p> <p>For a sample of quarters, inspected the results of management's review to confirm that code developers were not permitted update access to production system environments, applications and databases and migration of the approved application programs and database changes were performed by production control staff who are separate to the code development team.</p> <p>No exceptions were identified.</p>
34.5	Logically separate development, testing, and production environments have been established and are restricted to authorised individuals.	<p>Inspection</p> <p>For a sample of applications, inspected evidence that the development, testing and production environments were logically separated and restricted to authorised individuals.</p> <p>No exceptions were identified.</p>
34.6	For self-maintained applications, Version Control Software is in place to ensure that the correct version of the application program is being changed and the correct version of the application programs are being released to the production environment upon testing and approval.	<p>Observation</p> <p>For self-maintained applications, observed that version control software was in place to confirm that the correct version of the application program was being changed upon approval of a change request and that the correct version of the application programs were released to the production environment upon testing and approval.</p> <p>No exceptions were identified.</p>

34.7	On an annual basis, reviews are performed over third-party service providers ISAE 3402 (or equivalent) Internal Control Reports at the control objective level and user considerations are evaluated.	Inspection For a sample of third-party service providers inspected the results of management's review of ISAE 3402 (or equivalent) internal Control Reports to confirm that it was performed, and user considerations were evaluated. No exceptions were identified.
------	---	---

Recovery from Processing Interruptions

Columbia Threadneedle Investments EMEA's data is replicated between its primary and secondary data centres on a regular basis, to enable alternate recovery positions. Any failures identified during these replications are investigated, addressed, and the replication remediated. Management performs periodic reviews of the failures, to confirm that staff are following the required procedures, by raising the failed replications jobs as incidents and tracking them through to successful resolution within the Service Management system. Periodic testing of off-site backup recovery is undertaken to assure recoverability.

35	Controls provide reasonable assurance that in-scope systems and data are backed up and tested such that they can be restored completely and within agreed timescales	
	Control Procedure	PwC Testing Procedures and Results
35.1	Backup Data is replicated between the primary and secondary data centres regularly to enable alternate recovery position.	Observation For a sample of applications observed the replication configuration settings on the backup monitoring and reporting tool to confirm that backup data was replicated regularly from the primary to the secondary data centre. No exceptions were identified.
35.2	Data recoverability and restoration testing is performed on an annual basis. Noted issues are investigated and resolved in a timely manner.	Inspection For a sample of systems, inspected the results of the recoverability and restoration testing to confirm that data recoverability and restoration testing was performed at least on an annual basis and any issues were investigated and resolved in a timely manner, in accordance with internal policy. No exceptions were identified.
35.3	On a quarterly basis, management performs a review to confirm that failures of replication jobs are raised as issues and tracked through to resolution within the incident management system.	Inspection For a sample of quarters, inspected the results of management's review to confirm that replication processing failures were raised as issues and tracked through to resolution within the Incident Management System. No exceptions were identified.

35.4	On an annual basis, management monitors the DR exercise recovery results. Issues are tracked to resolution.	Inspection Inspected the results of management's monitoring of DR exercise recovery results to ensure that this was performed and issues were tracked to resolution. No exceptions were identified.
------	---	--

The goal of the Columbia Threadneedle Investments EMEA Incident Management process is to recover standard service operations as quickly as possible and to minimise the adverse impact on business operations so that the best possible levels of service quality and system availability are maintained. Processing incidents are identified and, either manually or automatically, entered into the Service Management system, where they are prioritised by severity. On a monthly basis, the Problem Management team reviews a sample of resolved P1, P2, P3 and P4 Incident tickets to confirm the incident ticket was prioritised based on the severity of the issue; documented with an Assignment Group, Configuration Item, and Close Notes in accordance with the Incident Management Process; and that each P1 Incident ticket is related to a Problem ticket as per the control process. Incident tickets are assigned to the appropriate Technology support group for resolution, based on the type of incident, and resolution is documented in the ticket record.

36	Controls provide reasonable assurance that problems and incidents relating to In-scope systems are identified and resolved within agreed timescales	
	Control Procedure	PwC Testing Procedures and Results
36.1	Monthly, the Incident Management team reviews a sample of Resolved P1, P2, and P3 Incident Tickets to confirm the incident ticket was prioritised based on the severity of the issue; documented with an Assignment Group, Configuration Item, and Close Notes in accordance with the Incident Management Process; and, that each P1 Incident Ticket is related to a Problem ticket. Discrepancies identified are resolved by the Incident Management team with input from the Incident Assignment Group.	Inspection For a sample of monthly incident ticket review, inspected results of the management review to confirm incidents were prioritised, documented with relevant fields and that each P1 incident ticket is related to a problem ticket. Any discrepancies identified are resolved by the incident management team. No exceptions were identified.
36.2	Monthly, the Problem Management team reviews a sample of Resolved Problem Tickets related to P1 Incidents to confirm these problem tickets are documented appropriately in accordance with the Problem Management Process. Discrepancies identified are resolved by the Problem Management team with input from the Problem Assignment Group.	Inspection For a sample of monthly problem tickets review, inspected results of the management review to confirm problems went through the problem management process. Any discrepancies identified are resolved by the problem management team. No exceptions were identified.

Columbia Threadneedle run two London data centres. This provides a production environment with replication to a disaster recovery data centre. Some applications are balanced between the data centres to give immediate resiliency; however, in the total loss of the production data centre a Virtualisation / SAN based recovery can be completed.

37	Controls provide reasonable assurance that IT related Disaster Recovery Plans are documented, updated, approved and tested	
	Control Procedure	PwC Testing Procedures and Results
37.1	Annually, the Disaster Recovery Plan is reviewed, updated and approved by management.	Inspection Inspected results of Disaster Recovery Plan review to confirm that it was updated and approved by management. No exceptions were identified.
37.2	On an annual basis, management monitors the DR exercise recovery results. Issues are tracked to resolution.	Inspection Inspected the results of management's monitoring of DR exercise recovery results to ensure that this was performed and issues were tracked to resolution. No exceptions were identified.

Columbia Threadneedle operates a comprehensive exercise schedule focusing on all critical functions of the recovery plan.

Managing and monitoring compliance and outsourcing

The Enterprise Vendor Management Requirements provide details, processes and expectations for employees who are responsible for managing third party vendor relationships as part of their role at Ameriprise. The goal of these requirements is to ensure Columbia Threadneedle maintains effective vendor relationships across the organization by consistently managing the contractual performance of each vendor.

The day-to-day business operations with vendors are managed at the business level at which the services are performed. The Enterprise Vendor Management Organization (EVMO), within Chief Risk Officer Organization, exists to aid business owners by driving consistency in Vendor Management standards and offering support.

38	Controls provide reasonable assurance that outsourced activities provided by Subservice Organisations are governed by contracts and service level agreements that are authorised and subject to regular review and that the services provided by Subservice Organisations are regularly monitored and assessed against the standards set out in the service level agreements	
	Control Procedure	PwC Testing Procedures and Results
38.1	On an annual basis, reviews are performed over third-party service providers ISAE 3402 (or equivalent) Internal Control Reports at the control objective level and user considerations are evaluated.	Inspection For a sample of third-party service providers inspected the results of management's review of ISAE 3402 (or equivalent) internal Control Reports to confirm that it was performed, and user considerations were evaluated. No exceptions were identified.

38.2	Quarterly, the Enterprise Vendor Management Office (EVMO) monitors Technology vendor records to confirm they are populated in accordance with the Enterprise Vendor Management Requirements. Discrepancies are communicated to the Engagement or Vendor Owners who are responsible for updating the vendor records. Unresolved discrepancies are reported to the CIO for follow-up and resolution.	Inspection For a sample of quarterly EVMO reviews, inspected results of the review and escalation to the CIO when needed, to confirm that required follow ups and resolutions were made. No exceptions were identified.
39.	Controls provide reasonable assurance that the physical IT equipment is maintained in a controlled environment	
	Control Procedure	PwC Testing Procedures and Results
39.1	On an annual basis, reviews are performed over third party service providers ISAE 3402 (or equivalent) internal Control Reports at the control objective level and user considerations are evaluated.	Inspection For a sample of third-party service providers inspected the results of management's review of ISAE 3402 (or equivalent) internal Control Reports to confirm that it was performed, and user considerations were evaluated. No exceptions noted.
39.2	Quarterly, the Enterprise Vendor Management Office (EVMO) monitors Technology vendor records to confirm they are populated in accordance with the Enterprise Vendor Management Requirements. Discrepancies are communicated to the Engagement or Vendor Owners who are responsible for updating the vendor records. Unresolved discrepancies are reported to the CIO.	Inspection For a sample of quarterly EVMO reviews, inspected results of the review and escalation to the CIO when needed, to confirm that required follow ups and resolutions were made. For a sample of vendors inspected the results of the Enterprise Vendor Management Office reviews to confirm that they were performed and any unresolved discrepancies were escalated to the Control owner or CIO for follow up and resolution No exceptions noted.

Section III – Management Responses

Management response to control exceptions

17	Controls provide reasonable assurance that cash is managed with regard to diversification of risk and security of funds.		
18	Controls provide reasonable assurance that client investments and cash are managed in accordance with investment objectives and monitored for compliance with investment guidelines and restrictions.		
20	Controls provide reasonable assurance that counterparty exposures are monitored for compliance with the firm's limits and guidelines.		
Control Ref	Control Procedure	Service Auditor's Test of Control Procedure	Management Response
17.2, 18.6, 20.9	On a daily basis, a member of the Mandate Compliance Team extracts and reviews an end-of-day report from Aladdin containing all live violations and a rationale is added for any alerts which are pending action or are closed without a future test date. This review is evidenced via email sign-off.	<p>Inspection For a sample of days, inspected evidence of the review of the end-of-day report from Aladdin containing all live violations and confirmed that a rationale was added for any alerts which were pending action or were closed without a future test date and an email was sent to Mandate Compliance team for proof of review.</p> <p>Management-identified exception: Management self-identified two instances during the period where the end of day check (Control 18.6) had not been performed: i) End of day review for 9 Feb 23 ii) End of day review for 26 July 2023 (additional MIE communicated to PwC on 10/08/2023)</p> <p>Inspection Confirmed through inspection of one end of day report from Aladdin containing all live violations of manual and automated rules triggered the previous day that the data contained within it completely and accurately reflected the data held on Aladdin.</p> <p>No exceptions were identified.</p>	<p>Management completed a review of all business days in the ISAE period to confirm that there were no further instances of this control not being performed as required.</p> <p>Management issued reminders to team members following the identification of the instances noted in the ISAE period.</p>

17.3, 18.7, 20.10	<p>On a daily basis, the Mandate Compliance monitoring team are responsible for reviewing all new and repeating alerts generated by the overnight batch process in Aladdin. All new alerts generated (i.e., those alerts which have an age of 1 day) are subject to a second review by another member of the Mandate Compliance monitoring team. Both the first and second review of new alerts are recorded within Aladdin.</p> <p>A senior member of the Mandate Compliance monitoring team.</p>	<p>Inspection For a sample of new alerts, inspected screenshots from Aladdin to confirm they were subject to a secondary review by a separate senior team member of the Mandate Compliance monitoring team.</p> <p>Management-identified exception: Management self-identified 3 instances during the period where the 4-eyes review of new alerts for the day (had not been performed.</p> <p>Details of missed 4 eyes reviews (exceptions in control 18.7) and the end of day check which failed to identify the issue (exceptions in control 18.6):</p> <ul style="list-style-type: none"> i) 1 new alert on 26 Jan 23 ii) 1 new alert on 20 Mar 23 ii) 1 new alert on 24 Mar 23 	<p>Management completed a review of all business days in the ISAE period to confirm that there were no further instances of this control not being performed as required.</p> <p>Management issued reminders to all team members following the identification of the instances noted in the ISAE period.</p>
----------------------------------	--	--	--

23	Controls provide reasonable assurance that client reporting in respect of portfolio valuation, transactions, holdings and income is complete and accurate and provided within agreed timescales.		
Control Ref	Control Procedure	Service Auditor's Test of Control Procedure	Management Response
23.4	<p>October 1, 2022 – April 30, 2023 Monthly, a series of data quality checks is performed by Information Management over data transferred from the portfolio management system to client reporting systems. Discrepancies are researched and resolved. Client Reporting is notified after discrepancies have been resolved.</p> <p>May 1, 2023 – September 30, 2023 Monthly, a series of data quality checks is performed by Information Management over data transferred from the portfolio management system to client reporting systems. Discrepancies are researched and resolved. Client Reporting is notified after discrepancies have been resolved. Failed data quality checks are monitored daily for completeness of research and resolution.</p>	<p>October 1, 2022 – April 30, 2023 Inspection For a sample of months, inspected quality checks were performed by Information Management for data transfers between portfolio management systems and client reporting systems. Further validated that discrepancies are researched and resolved.</p> <p>Exceptions noted.</p> <p>Management self-identified that 3 out of a population of 422 failed data quality checks were not adequately researched and resolved.</p> <p>No additional exceptions noted from PwC testing.</p> <p>May 1, 2023 – September 30, 2023 Inspection For a sample of months, inspected quality checks were performed by Information Management for data transfers between portfolio management systems and client reporting systems, to determine whether discrepancies were researched and resolved.</p> <p>No exceptions were identified.</p> <p>Inspection For a sample of quality checks, inspected management's daily monitoring to determine whether it was performed for completeness of research and resolution of failed data quality checks.</p> <p>No exceptions were identified.</p> <p>Reperformance For a sample of failed quality checks, reperformed management's daily monitoring to determine whether a failure alert was sent for each failed quality check and that the daily quality check monitoring was performed to match the failure with an incident ticket and email alert.</p> <p>No exceptions were identified.</p>	<p>Management acknowledges the self-identification of 3 Data Quality (DQ) Check alerts that was not researched and resolved timely as ServiceNow failed to generate an incident ticket to route the Management Record (IMR) to the appropriate support group. Upon further research, it was verified that these 3 DQ check alerts did not point to any real issues with the data files that had any negative downstream impacts on client reporting.</p> <p>As of May 1, 2023, management enhanced the control activity through implementing a daily process to monitor for data quality checks that failed to generate automated incident tickets and route them via email alerts to those responsible for research and resolution. Additional improvements to Dynamo DB to Service Now interface application are also underway to generate timely notification of ServiceNow incident ticket generation fails.</p> <p>Additionally, there is a Mitigating Control (23.1) in place that is designed to detect issues with client reports prior to report distribution. Control 23.1 requires secondary review and signoff of each report by a Client Reporting member before they can be distributed to clients.</p>

Section IV – Information provided by the Service Auditor

This report on the controls surrounding the provision of investment management services to institutional clients is intended to provide interested parties with information sufficient to understand the flow of transactions for the processes and control procedures in place at Columbia Threadneedle Investments EMEA.

The review of Columbia Threadneedle Investments EMEA controls was restricted to the overview in Section I and the control objectives and the controls set forth by the Company in Section I of this report that Columbia Threadneedle Investments EMEA believes are the relevant control objectives and controls, and was not extended to procedures in effect at customer or other service or subservice organisation locations. This report has been prepared according to the guidance contained in AAF 01/20, Assurance Reports on Internal Controls of Service Organisations Made Available to Third Parties and ISAE 3402, Assurance Reports on Controls at a Service Organization. It is each interested party's responsibility to evaluate this information in conjunction with user controls in place for each user entity as outlined in "Complementary User Entity Controls" and other user entity controls, in order to assess the overall internal control. If an effective user entity internal control is not in place, the control procedures applied at Columbia Threadneedle Investments EMEA may not compensate for its absence. The objectives of internal controls are to provide reasonable, but not absolute, assurance as to the reliability of financial records for maintaining accountability for assets. The concept of reasonable assurance recognises that the cost of a control should not exceed the benefits derived and recognises that the evaluation of these factors necessarily requires estimates and judgments by management.

As part of the review of the Company's controls we performed a variety of tests, each of which provided different levels of audit satisfaction. The combined results of these tests provided the basis for understanding the controls and whether the controls surrounding the investment management services that the Company represented as placed in operation were actually designed, in place and operating effectively for the period 1 October 2022 to 30 September 2023.

Control Environment

The control environment represents the collective effect of various factors on establishing, enhancing or mitigating the effectiveness of specific controls. In addition to the tests of specific controls described below, our procedures included tests of, or considered the relevant elements of, the Company's control environment including:

- The Company's organisational structure and approach to segregation of duties;
- Management control methods;
- Personnel policies and practices; and
- Departments with oversight functions.

Our tests of the control environment included the following procedures, to the extent we considered necessary: (1) a review of Columbia Threadneedle Investment's organisational structure, including segregation of functional responsibilities, policy statements, accounting and processing manuals, and personnel policies; (2) discussions with management, operations, administrative and other personnel who are responsible for developing, ensuring adherence to and applying controls; and (3) observations of personnel in the performance of their assigned duties.

The control environment was considered in determining the nature, timing and extent of the testing of the operation of the controls relevant to achievement of the control objectives.

Control Procedures

Our tests of the operating effectiveness of controls included such tests as were considered necessary in the circumstances to evaluate whether those controls and the extent of compliance with them, are sufficient to provide reasonable, but not absolute, assurance that the specified control objectives were achieved during the period from 1 October 2022 to 30 September 2023. Our testing of the operating effectiveness of controls was designed to cover a representative number of transactions and controls throughout the period from 1 October 2022 to 30 September 2023, for each of the controls listed in the matrices in Section II, which are designed to achieve the specified control objectives.

In selecting particular tests of the operating effectiveness of controls, the following were considered: (a) the nature of the items being tested; (b) the types and competence of available evidential matter; (c) the nature of the control objectives to be achieved; (d) the assessed level of control risk; and (e) the expected efficiency and effectiveness of the test. For any tests noted as having been performed in the test environment, procedures were completed to validate that the test instance was identical to the current production environment at the time of testing. Additionally, observation and inspection procedures were performed as it relates to system-generated reports, queries, and listings to assess the completeness and accuracy (reliability) of the information utilised in the performance of our testing of the control activities.

Tests performed over the operating effectiveness of the control activities were performed on a judgmental basis and are described below:

Tests	Description
Inquiry (Corroboration)	<p>Inquired of appropriate personnel. Inquiries seeking relevant information or representation from personnel were conducted to obtain, among other factors:</p> <ul style="list-style-type: none"> ■ Knowledge and additional information regarding the control, policy or procedure; and ■ Corroborating evidence of the control, policy or procedure. <p>As inquiries were performed for substantially all controls, the test was not listed individually for every control shown in the matrices in Section II.</p>
Observation	Observed the application or existence of specific controls as represented.
Inspection/ Examination	<p>Inspected documents and records indicating performance of the control. This may include:</p> <ul style="list-style-type: none"> ■ Examination of source documentation and authorizations to verify propriety. ■ Examination of documents or records for evidence of performance, such as existence of initials or signatures. ■ Examination of documentation, such as operations manuals, flow charts, job descriptions and user profiles.
Reperformance	Reperformed the control or processing to determine the accuracy of its operation, including obtaining evidence of the arithmetical accuracy and correct processing of transactions by recomputing the application computation.

Sample Sizes

The sample sizes that have been applied in testing control procedures, depending on the frequency the control is applied, and the assessed level of control risk are set out in the table below:

Frequency of control	Number of items tested
Annual	1
Quarterly	2
Monthly	2, 4, 5
Weekly	5, 10, 15
Daily	20, 30, 40
Multiple times per day	25, 45, 60

Use of Management Testing

For part of our testing, we relied upon testing performed by management. In addition to reviewing the level of skill and experience of management testers and the objectivity and independence of the controls which they were responsible for testing, we also reviewed the working papers for those management tests which we placed reliance upon, and in certain cases reperformed the work performed by management to ensure that the work performed was equivalent to work we would have performed ourselves were we to have performed the testing. We have identified in Section II using the heading "Reliance on Risk and Control Services team", those tests where we have relied upon management testers.

Appendix I – Prospective Client Disclaimer Letter



PRIVATE AND CONFIDENTIAL

The Directors
Threadneedle Asset Management Limited and
Threadneedle International Limited
Cannon Place
78 Cannon Street
London
EC4N 6AG

Dear Sirs or Madams,

**RELEASE OF THE 2023 ISAE 3402 / AAF 01/20 REPORT TO PROSPECTIVE CLIENTS OF
THREADNEEDLE ASSET MANAGEMENT LIMITED AND THREADNEEDLE INTERNATIONAL
LIMITED, TOGETHER REFERRED TO AS “COLUMBIA THREADNEEDLE” OR THE “SERVICE
ORGANISATIONS”.**

The 2023 ISAE 3402 / AAF 01/20 report which covers the internal controls relating to investment management services for institutional investment management services for segregated mandates provided by Columbia Threadneedle (the “service organisations”) for the year ended 30 September 2023, has been prepared by the directors of the service organisations principally for the purposes of providing information to organisations who were customers at 30 September 2023 or any time during the preceding year. You have asked us to agree to you providing to prospective customers, i.e. organisations that were not customers at 30 September 2023 or the preceding year, a copy of the 2023 ISAE 3402 / AAF 01/20 report which includes our service auditor’s assurance report (“our assurance report”) dated 19 December 2023.

We confirm that we are agreeable to you so doing on the clear understanding that our assurance report was addressed to you and was prepared on your instructions as set out in our engagement letter dated 12th June 2023 and therefore items of possible interest to prospective customers may not have been specifically addressed by the 2023 ISAE 3402 / AAF 01/20 report or the work supporting our assurance report. Nor does PricewaterhouseCoopers LLP warrant or represent that the information in the 2023 ISAE 3402 / AAF 01/20 report or work done in connection with our assurance report is appropriate for the interests or purposes of prospective customers. For the foregoing reasons, the 2023 ISAE 3402 / AAF 01/20 report cannot in any way serve as a substitute for enquiries and procedures that prospective customers would (or should) undertake and judgements they should make for the purpose of satisfying themselves regarding any matters of interest to them. Furthermore, we accept no duty or responsibility and deny any liability to prospective customers or to any other third party in relation to our assurance report or otherwise, whether or not the 2023 ISAE 3402 / AAF 01/20 report or our assurance report therein influences the decision or action of any prospective customer or any other party.

Prospective customers are also bound by a duty of confidentiality to PricewaterhouseCoopers LLP, as well as to you. Consequently, the 2023 ISAE 3402 / AAF 01/20 report, and information obtained from it, must not be made available or copied, in whole or in part to any other person without our prior written permission which we may, at our discretion, grant, withhold or grant subject to conditions (including conditions as to legal responsibility or absence thereof).


PricewaterhouseCoopers LLP, 7 More London Riverside, London, SE1 2RT
T: +44 (0) 20 7583 5000, F: +44 (0) 20 7212 7500, www.pwc.co.uk

PricewaterhouseCoopers LLP is a limited liability partnership registered in England with registered number OC303525. The registered office of PricewaterhouseCoopers LLP is 1 Embankment Place, London WC2N 6RH. PricewaterhouseCoopers LLP is authorised and regulated by the Financial Services Authority for designated investment business.

Notwithstanding our consent to the release of the 2023 ISAE 3402 / AAF 01/20 report to prospective customers, our assurance report remains addressed to you and it is a matter for you to decide whether the release of the 2023 ISAE 3402 / AAF 01/20 report is appropriate in the circumstances.

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

Yours faithfully

A handwritten signature in dark ink that reads "PricewaterhouseCoopers LLP". The signature is written in a cursive, flowing style.

PricewaterhouseCoopers LLP

Appendix II – Important information

The information contained in this document is confidential and should not be disclosed to third parties. The information is provided on the basis that the recipient will maintain its confidence unless it is required to disclose it by applicable law or regulations. It is also our view that certain information contained in this document may amount to a trade secret, and could, if disclosed, prejudice our commercial interests.

If you intend to disclose any of the information contained in this document for any reason, including, but not limited to, in response to a request under the Freedom of Information Act, you agree to notify and consult with Columbia Threadneedle Investments prior to making any such disclosure, so that Columbia Threadneedle Investments can ensure its rights are protected. Any entity or person with access to this information shall be subject to this confidentiality statement.

Columbia Threadneedle Investments is a brand name, and both the Columbia Threadneedle Investments name and logo are trademarks or registered trademarks of the Columbia Threadneedle group of companies.



To find out more visit columbiathreadneedle.com

Important information: Threadneedle Investment Services Limited, ISA Manager, Authorised Corporate Director and Unit Trust Manager. Registered No. 3701768. Registered in England and Wales. Registered Office: Cannon Place, 78 Cannon Street, London EC4N 6AG. Authorised and regulated by the Financial Conduct Authority. Columbia Threadneedle Investments is the global brand name of the Columbia and Threadneedle group of companies. columbiathreadneedle.com.