

Morgans Financial Limited

Wealth+ Managed Portfolio Service

Report over the Investment Administration Controls in accordance with GS 007 for the period 1 July 2022 to 30 June 2023

Morgans Financial Limited
Wealth+ Managed Portfolio Service

Report over the Investment Administration Controls in accordance with GS 007
30 June 2023

Contents

1. Independent Service Auditor’s Assurance Report..... 3

2. Morgans Financial Limited’s Assertion on the Wealth+ Managed Portfolio Service System..... 5

3. Description of the Wealth+ Managed Portfolio Service System Accompanying Morgans Financial Limited Management’s Assertion..... 7

4. Service Auditor’s Description of the Nature, Timing and Extent of Tests Applied to Controls..... 10

5. Control Objectives, Related Controls, Audit Procedures to Test Operating Effectiveness of Allied Controls and Results of Procedures 11

5.1 Accepting Clients..... 11

5.2 Authorising and processing transactions 12

5.3 Maintaining financial and other records 13

5.4 Monitoring Compliance..... 15

5.5 Reporting to clients..... 16

5.6 Taxation 16

5.7 Restricting access to systems and data..... 18

5.8 Authorising and processing transactions 25

5.9 Safeguarding assets..... 35

5.10 Maintaining and developing systems hardware and software 36

5.11 Recovering from processing interruptions 40

5.12 Monitoring compliance 44

5.13 Monitoring subservice organisations 47

1 Independent Service Auditor's Assurance Report

on the Description of Controls over the Wealth+ Managed Portfolio Service, their Design and Operating Effectiveness

To: Morgans Financial Limited

Scope

We have been engaged to report on Morgans Financial Limited's description as set out in sections 3 and 5 of its Wealth+ Managed Portfolio Service system provided to Morgans Financial Limited's clients throughout the year 1 July 2022 to 30 June 2023 (the description), and on the design and operations of those controls related to the control objectives stated in the description.

Morgans Financial Limited's Responsibilities

Morgans Financial Limited is responsible for: preparing the description and accompanying assertion as set out in section 2, including the completeness, accuracy and method of presentation of the description and assertion; providing the Wealth+ Managed Portfolio Service covered by the description; stating the control objectives, including relevant control objectives for the Wealth+ Managed Portfolio Service as outlined in AUASB Guidance Statement GS 007 *Audit Implications of the Use of Service Organisations for Investment Management Services*, and designing, implementing and effectively operating controls to achieve the stated control objectives.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on Morgans Financial Limited's description and on the design and operation of controls related to the control objectives stated in that description based on our procedures. We conducted our engagement in accordance with Standard on Assurance Engagements ASAE 3402 *Assurance Reports on Controls at a Service Organisation* and with reference to Guidance Statement GS 007 *Audit Implications of the Use of Service Organisations for Investment Management Services*. ASAE 3402 requires that we comply with relevant ethical requirements and plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented and the controls are suitably designed and operating effectively.

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 disclosures in the service organisation's description of its system, and the design and operating effectiveness of controls. The procedures selected depend on our judgement, including the assessment of the risks that the description is not fairly presented, and that controls are not suitably designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved.

An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the objectives stated therein, and the suitability of the criteria specified by the service organisation and described in sections 3 and 5.

In evaluating the suitability of the objectives stated in the description, we have determined whether each of the minimum control objectives provided in GS 007 for the Wealth+ Managed Portfolio Service is included, or, if any of the minimum objectives are omitted or amended, that the reason for the omission or amendment is adequately disclosed in the description.

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

Limitations of Controls at a Service Organisation

Morgans Financial Limited's description is prepared to meet the common needs of a broad range of clients and their auditors and may not, therefore, include every aspect of the system that each individual client may consider important in its own particular environment. Also, because of their nature, controls at a service organisation may not prevent or detect all errors or omissions in processing or reporting transactions. Also, the projection of any evaluation of effectiveness to future periods is subject to the risk that controls at a service organisation may become inadequate or fail.

Opinion

Our opinion has been formed on the basis of the matters outlined in this report. The criteria we used in forming our opinion are those described in section 4 of this report. In our opinion, in all material respects:

- a) the description fairly presents the Wealth+ Managed Portfolio Service system as designed and implemented throughout the period from 1 July 2022 to 30 June 2023;
- b) the controls related to the control objectives stated in the description were suitably designed throughout the period from 1 July 2022 to 30 June 2023; and
- c) the controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period from 1 July 2022 to 30 June 2023.

Description of Tests of Controls

The specific controls tested and the nature, timing and results of those tests are listed in sections 4 and 5 of this report.

Intended Users and Purpose

This report and the description of tests of controls in sections 4 and 5 of this report are intended only for clients who have used Morgans Financial Limited's Wealth+ Managed Portfolio Service system, and their auditors, who have a sufficient understanding to consider it, along with other information including information about controls operated by clients themselves, when assessing the risks of material misstatements of clients' financial reports/statements.

Pitcher Partners
PITCHER PARTNERS

J. Evans
JASON EVANS
Partner

Brisbane, Queensland
1 August 2023

2. Morgans Financial Limited's Assertion on the Wealth+ Managed Portfolio Service System

The accompanying description has been prepared for clients who have used the Wealth+ Managed Portfolio Service system and their auditors who have a sufficient understanding to consider the description, along with other information including information about controls operated by clients themselves, when assessing the risks of material misstatements of clients' financial reports/statements. Morgans Financial Limited confirms that:

- a) The accompanying description set out in sections 3 and 5 of this report fairly presents the Wealth+ Managed Portfolio Service system for processing clients' transactions throughout the period 1 July 2022 to 30 June 2023. The criteria used in making this assertion were that the accompanying description:
- i) Presents how the system was designed and implemented, including:
 - The types of services provided, including, as appropriate, classes of transactions processed;
 - The procedures, within both information technology and manual systems, by which those transactions were initiated, recorded, processed, corrected as necessary, and transferred to the reports prepared for clients;
 - 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 was transferred to the reports prepared for clients;
 - How the system dealt with significant events and conditions, other than transactions;
 - The process used to prepare reports for clients;
 - Relevant control objectives and controls designed to achieve those objectives, including the control objectives for investment administration provided in Guidance Statement 007 *Audit Implications of the Use of Service Organisations for Investment Management Services* except for two control objectives which have been omitted for the reasons set out in section 5;
 - Controls that we assumed, in the design of the system, would be implemented by clients, and which, if necessary to achieve control objectives stated in the accompanying description, are identified in the description along with the specific control objectives that cannot be achieved by ourselves alone; and
 - Other aspects of our control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls that were relevant to processing and reporting clients' transactions; and
 - ii) Includes relevant details of changes to the system during the period 1 July 2022 to 30 June 2023; and
 - iii) Does not omit or distort information relevant to the scope of the system being described, while acknowledging that the description is prepared to meet the common needs of a broad range of clients and their auditors and may not, therefore, include every aspect of the system that each individual client may consider important in its own particular environment; and

- b) The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period 1 July 2022 to 30 June 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;
 - ii) 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
 - iii) The controls were consistently applied as designed, including manual controls that were applied by individuals who have the appropriate competence and authority, throughout the period 1 July 2022 to 30 June 2023.



Signed on behalf of the directors of Morgans Financial Limited
Jeffrey Oates - Director



Signed on behalf of the directors of Morgans Financial Limited
Daniel Spokes - Director

Brisbane, Queensland
1 August 2023

3. Description of the Wealth+ Managed Portfolio Service System Accompanying Morgans Financial Limited Management's Assertion

Services provided

Morgans Financial Limited provides its clients with investment administration services through its Wealth+ Managed Portfolio Service. The Wealth+ Managed Portfolio Service collects and records investment information, including security trades, dividends and distributions and interest payments and supplies clients with regular reports including annual taxation statements detailing the asset portfolio held and all relevant transactions for the year. These may include distributions and relevant tax components, dividends and their associated taxation credits, realised and distributed capital gains and losses and deductible expenses such as fees and interest paid on loans. It also provides advice on the tax treatment of corporate actions processed during the year.

The System

The stated internal control objectives and related controls included in this report apply to Morgans Financial Limited's operations as they relate only to Wealth+ Managed Portfolio Services. Specifically excluded from this report are controls within individual systems, controls executed at client premises and other services provided by Morgans Financial Limited.

The effectiveness of controls performed by clients of Morgans Financial Limited should also be considered as part of the overall system of controls relating to Morgans Financial Limited's Wealth+ Managed Portfolio Services.

Introduction

Set out below is a description of the System for the service offering covered by this report. It should be read in conjunction with the remainder of this report.

It is noted that not all clients utilise the full range of services offered by Morgans Financial Limited. As such, the description is only relevant to each client to the extent they use the relevant service.

Recording and processing of new account setup

A number of assessments are required to be completed prior to signing agreements with new clients. The completion of all relevant assessments is monitored by Morgans Financial Limited. Based on the agreement with the client, account opening forms are then completed by the client. The client account is setup in the administration system as per the account opening form, and a secondary check is performed over the accuracy of the account information.

Initiation of transactions (static data, applications, switches, redemptions)

Instructions are received from clients to initiate transactions and to update client account standing data, and are subject to authentication prior to initiation. Instructions are authenticated through sight verification of the client's signature on the instruction against the original signature recorded for that client on the Wealth+ Client Agreement.

Recording, processing and correction of applications and redemptions

Instructions to process applications / redemptions are received electronically, authenticated and routed to the appropriate team. Applications are processed in the administration system, and redemption details are automatically produced from the administration system and these are sent to the relevant fund manager.

Payments received in settlement of redemptions are identified, reconciled and recorded in the administration system.

Movements as recorded on fund manager statements are reconciled to transactions processed in the administration system.

Recording, processing and notification of corporate actions

On a daily basis corporate actions are processed based on the security holdings recorded in the administration system. Details of each corporate action are checked against external information vendors for completeness, accuracy and validity, and the administration system is updated as appropriate. The positions recorded in the administration system are compared to the positions recorded via external security holdings systems.

Recording, processing and correction of security valuation and unit pricing

On a regular basis, asset prices are requested and received back from external information vendors. Following the application of prices to the system, a review of any unpriced assets, stale prices or price movements outside of predefined tolerances is performed.

The pricing updates are automatically applied to security holdings in the administration system.

Recording, processing and correction of management fees

Management fees are recorded in the administration system and are accrued in line with the agreed rates. Monthly / Quarterly fees are raised against accounts recorded in the administration systems and monies are withdrawn from clients' cash management accounts.

Client reporting

Daily reconciliations are performed which identifies any variances between the administration system and external cash and security holdings systems. Reports are produced automatically from the administration system and used to populate predefined reporting templates.

Significant Events

As set out in control objective 13 of the report, Morgans has a process in place that governs the escalation, investigation and reporting of reportable incidents and errors.

Errors are identified through a number of detective mechanisms such as completeness checks, reconciliations, and through client review of reports or transactions as set out in other sections of this report.

Escalation paths have been clearly defined and are commensurate with the significance of the incident, and also provide guidance for the reporting of incidents to our clients.

The defined process enables a consistent approach to managing incidents and promotes an open communication culture with a continual focus on process improvement.

Material Changes in our System during the period

Morgans Financial Limited is a dynamic business which regularly refines its systems and processes to meet the requirements of clients, address market changes and improve efficiency and effectiveness of controls.

Morgans Financial Limited can confirm that during the 12 month period covered by this report there were no significant changes to our systems.

The controls which were in operation at Morgans Financial Limited throughout the period from 1 July 2022 to 30 June 2023, or during a lesser period where specified, to ensure that the identified control objectives over the Wealth+ Managed Portfolio Service are described in section 5 of this report.

4. Service Auditor's Description of the Nature, Timing and Extent of Tests Applied to Controls

Our audit has been conducted to enable us to form an opinion on the following objectives:

- a) the description fairly presents the Wealth+ Managed Portfolio Service system as designed and implemented throughout the period from 1 July 2022 to 30 June 2023;
- b) the controls related to the control objectives stated in the description were suitably designed throughout the period from 1 July 2022 to 30 June 2023; and
- c) the controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period from 1 July 2022 to 30 June 2023.

The nature, timing, and extent of tests applied to controls and the results setting out any exceptions to the objectives a), b) and c) are described in section 5 of this report. For each control objective Pitcher Partners carried out the following procedures over Morgans Financial Limited's Wealth+ Managed Portfolio Service control environment:

- Through observation and enquiry, we confirmed our understanding of the Wealth+ Managed Portfolio Service system description;
- Through observation and enquiry, we assessed whether the controls in relation to the Wealth+ Managed Portfolio Service were suitably designed to meet the control objectives; and
- Through enquiry, inspection, observation and re-performance we assessed whether the controls operated effectively throughout the period 1 July 2022 to 30 June 2023 to meet the control objectives as defined by Morgans Financial Limited.

When performing the test of operating effectiveness of a control we applied the following sample sizes:

Control Type	Frequency of Control	Sample Size
Manual controls relating to Wealth+ process activities in IT processes	Daily or many times daily	24
	Monthly	2
	Quarterly	1
	Annually	1
Automated application controls	Not applicable	1

5. Control Objectives, Related Controls, Audit Procedures to Test Operating Effectiveness of Allied Controls and Results of Procedures

INVESTMENT ADMINISTRATION CONTROL OBJECTIVES

5.1 Accepting Clients

Control Objective	Related Control	Frequency	Procedure	Results
E.1 New accounts are set up completely and accurately in accordance with client agreements and any applicable regulations.	Checklists are used to ensure all steps of the new client setup process are performed completely and accurately. This includes the New Client Set Up Checklist which ensures all required documents have been received and setup correctly in all required systems. A second person checks all data entry is correct and evidences this by signing the Application Data Check report.	Daily or many times daily	For a sample of clients who commenced with the Wealth+ Managed Portfolio Service during the year inspect the New Client Set Up Checklist and Application Data Check report for evidence that all required steps were completed and reviewed by a second person as evidenced by the signature on the Data Check report.	No exceptions noted.
E.2 Complete and authorised client agreements are established prior to initiating accounting activity.	1. Prior to obtaining sign off on a Wealth + Application data check the Wealth+ New Client Team ensures a signed Wealth+ Client Agreement is on file and the customer is marked as active.	Daily or many times daily	For a sample of clients who commenced with the Wealth+ Managed Portfolio Service during the year inspect that the account status is active and listed as an 'MPS' account and that the data check is done on or after the execution date of the Wealth+ Team	No exceptions noted.
	2. Wealth+ Client Agreements are required to be executed by two Wealth+ personnel from the authorised signatory list prior to activation of the account.	Daily or many times daily	For a sample of clients who commenced with the Wealth+ Managed Portfolio Service during the year obtain Wealth+ Client Agreements and inspect execution of the agreement by two authorised signatories of the Wealth+ team.	No exceptions noted.

5.2 Authorising and processing transactions

Control Objective	Related Control	Frequency	Procedure	Results
E.3 Portfolio transactions are recorded completely, accurately and on a timely basis.	1. On a daily basis, cash and security positions supplied by external cash account providers and security trading platforms are reconciled to holding positions recorded in the Wealth+ system using the automated RECON system. All exceptions are identified by the Reconciliation Team and forwarded to the appropriate Transaction Team member for remediation on a timely basis.	Daily or many times daily	For a sample of daily exception reports produced by the RECON system select an exception and inspect evidence of follow up with Transaction Teams and ensure remediation of the exception was on a timely basis.	No exceptions noted.
	2. The RECON system automatically uploads the data from the external cash account providers and security trading platforms with no manual input.	Daily or many times daily	Observe the automatic download of the data from the external sources and upload to the Wealth+ system.	No exceptions noted.
	3. For any unlisted transactions a computerised Wealth+ request is submitted by the client adviser to the Wealth+ Team which is actioned on a daily basis. The request is marked as complete once the Transaction Team has ensured the transaction was completely and accurately performed and recorded.	Daily or many times daily	For a sample of Wealth+ requests inspect that the request is marked as complete.	No exceptions noted.
E.4 Corporate actions are actioned, processed and recorded accurately and on a timely basis.	1. Corporate actions are recorded via a computerised Wealth+ request submitted by the client adviser. The request is marked as complete once the Transaction Team has ensured the transaction was completely and accurately performed and recorded.	Daily or many times daily	For a sample of Wealth+ requests inspect that the request is marked as complete.	No exceptions noted.
	2. On a daily basis, cash and security positions supplied by external cash account providers and security trading platforms are reconciled to holding positions recorded in the Wealth+ system using the automated RECON system. All exceptions are identified by the Reconciliation Team and forwarded to the appropriate Transaction Team member for remediation on a timely basis.	Daily or many times daily	For a sample of daily exception reports produced by the RECON system select an exception and inspect evidence of follow up with Transaction Teams and ensure remediation of the exception was on a timely basis.	No exceptions noted.

Control Objective	Related Control	Frequency	Procedure	Results
	3. The RECON system automatically uploads the data from the external cash account providers and security trading platforms with no manual input.	Daily or many times daily	Observe the automatic download of the data from the external sources and upload to the Wealth+ system.	No exceptions noted.
E.5 Expenses are appropriately authorised and recorded in accordance with the service level agreement and/or client instructions, on a timely basis.	As part of the client setup process, the fee schedule of the authorised Wealth+ Client Agreement is entered into the Wealth+ system by a member of the Wealth+ Billing Team and reviewed by a second member of the Wealth+ Billing Team.	Daily or many times daily	For a sample of clients who commenced with the Wealth+ Managed Portfolio Service during the year inspect the fee schedule form for evidence that the fees were entered into the system and checked by a second person.	No exceptions noted.

5.3 Maintaining financial and other records

Control Objective	Related Control	Frequency	Procedure	Results
E.6 Accounts are administered in accordance with client agreements.	Identified errors are recorded via a computerised Wealth+ request submitted by the client adviser. The request is marked as complete once the Transaction Team has ensured the transaction was completely and accurately performed and recorded.	Daily or many times daily	For a sample of Wealth+ requests inspect that the request is marked as complete.	No exceptions noted.
E.7 Changes to non-monetary static data (for example, address changes and changes in allocation instructions) are authorised and correctly recorded on a timely basis.	Changes to non-monetary static data is recorded via a computerised Wealth+ request submitted by the client adviser. The request is marked as complete once the Transaction Team has ensured the change was completely and accurately performed and recorded.	Daily or many times daily	For a sample of Wealth+ requests inspect that the request is marked as complete.	No exceptions noted.
E.8 Investment income and related tax are accurately calculated and recorded on a timely basis.	1. Dividend and distribution details received from external sources such as IRESS are entered by the Transaction Team when received. The calculation is checked for two clients accounts by a second person and the check is evidenced on the Dividend Security Activity Verification checklist.	Daily or many times daily	Select a sample of dividend and distribution payments made by listed entities and inspect the related Dividend Security Activity Verification checklist for evidence of second person check.	No exceptions noted.

Control Objective	Related Control	Frequency	Procedure	Results
	2. On a daily basis, cash and security positions supplied by external cash account providers and security trading platforms are reconciled to holding positions recorded in the Wealth+ system using the automated RECON system. All exceptions are identified by the Reconciliation Team and forwarded to the appropriate Transaction Team member for remediation on a timely basis.	Daily or many times daily	For a sample of daily exception reports produced by the RECON system select an exception and inspect evidence of follow up with Transaction Teams and ensure remediation of the exception was on a timely basis.	No exceptions noted.
	3. The RECON system automatically uploads the data from the external cash account providers and security trading platforms with no manual input.	Daily or many times daily	Observe the automatic download of the data from the external sources and upload to the Wealth+ system.	No exceptions noted.
E.9 Investments are valued using current prices obtained from independent external pricing sources, or an alternative basis in accordance with client agreements.	1. On a daily basis, pricing information is received from third parties (IRESS, Bloomberg and Morningstar) and automatically uploaded into the Wealth+ system.	Daily or many times daily	Observe the automatic download of the data from the external sources and upload to the Wealth+ system.	No exceptions noted.
	2. For securities which are not included in one of the third party data feeds, the pricing is updated monthly based on information received from the fund managers via various sources (e.g. website, direct phone calls, emails).	Daily or many times daily	For a sample of securities not included in the third party data feeds, obtain the pricing documentation retained from the fund manager and inspect that the price was entered correctly into Wealth+.	No exceptions noted.
E.10 Issue and cancellations of shares/units are recorded completely and accurately in the financial records and units on issue are regularly reconciled to data provided by registry.	1. On a daily basis, cash and security positions supplied by external cash account providers and security trading platforms are reconciled to holding positions recorded in the Wealth+ system using the automated RECON system. All exceptions are identified by the Reconciliation Team and forwarded to the appropriate Transaction Team member for remediation on a timely basis.	Daily or many times daily	For a sample of daily exception reports produced by the RECON system select an exception and inspect evidence of follow up with Transaction Teams and ensure remediation of the exception was on a timely basis.	No exceptions noted.
	2. The RECON system automatically uploads the data from the external cash account providers and security trading platforms with no manual input.	Daily or many times daily	Observe the automatic download of the data from the external sources and upload to the Wealth+ system.	No exceptions noted.

Control Objective	Related Control	Frequency	Procedure	Results
E.11 Cash and securities positions are completely and accurately recorded and reconciled to third party data on a timely basis.	1. On a daily basis, cash and security positions supplied by external cash account providers and security trading platforms are reconciled to holding positions recorded in the Wealth+ system using the automated RECON system. All exceptions are identified by the Reconciliation Team and forwarded to the appropriate Transaction Team member for remediation on a timely basis.	Daily or many times daily	For a sample of daily exception reports produced by the RECON system select an exception and inspect evidence of follow up with Transaction Teams and ensure remediation of the exception was on a timely basis.	No exceptions noted.
	2. The RECON system automatically uploads the data from the external cash account providers and security trading platforms with no manual input.	Daily or many times daily	Observe the automatic download of the data from the external sources and upload to the Wealth+ system.	No exceptions noted.
E.12 Reconciliations between different systems, including the investment ledger, general ledger and administration system, are performed on a timely basis.	1. On a daily basis, cash and security positions supplied by external cash account providers and security trading platforms are reconciled to holding positions recorded in the Wealth+ system using the automated RECON system. All exceptions are identified by the Reconciliation Team and forwarded to the appropriate Transaction Team member for remediation on a timely basis.	Daily or many times daily	For a sample of daily exception reports produced by the RECON system select an exception and inspect evidence of follow up with Transaction Teams and ensure remediation of the exception was on a timely basis.	No exceptions noted.
	2. The RECON system automatically uploads the data from the external cash account providers and security trading platforms with no manual input.	Daily or many times daily	Observe the automatic download of the data from the external sources and upload to the Wealth+ system.	No exceptions noted.

5.4 Monitoring Compliance

Control Objective	Related Control	Frequency	Procedure	Results
E.13 Errors are identified, notified to clients and rectified promptly in accordance with client agreements.	Identified errors are recorded via a computerised Wealth+ request submitted by the client adviser. The request is marked as complete once the Transaction Team has ensured the transaction was completely and accurately performed and recorded.	Daily or many times daily	For a sample of Wealth+ requests inspect that the request is marked as complete.	No exceptions noted.

5.5 Reporting to clients

Control Objective	Related Control	Frequency	Procedure	Results
E.15 Periodic reports to clients, including calculation of net asset value if required, are accurate and complete and distributed on a timely basis.	1. The Wealth+ system automatically compiles monthly (optional), quarterly and annual client reports from current Wealth+ data at the time of the creation of the report with no manual input required. At the end of the procedure, a report is created which compares expected portfolios against reports created.	Quarterly	Select one quarter and obtain the Quarter Report Checklist and ensure that the total expected portfolios agrees to the number of reports confirmed via the Reporting Portal.	No exceptions noted.
E.16 Annual reports and accounts are prepared in accordance with applicable laws and regulations.	1. The tax treatment for significant corporate transactions is verified by internal tax advisors and an independent review of the myTax references is performed by the Company's Management and Taxation Accountant who works independently of the internal Wealth+ tax team.	Annually	Obtain the Corporate Actions register and ensure tax calculations are reviewed by the internal tax team. Ensure that the annual independent review of the myTax references is performed by the Management and Taxation Accountant.	No exceptions noted.
	2. After generating the annual client reports, the Tax Team select a sample of reports and check accuracy and completeness prior to the reports being distributed to clients.	Quarterly	For a sample of annual client reports reviewed by the Tax Team inspect evidence of accuracy and completeness check.	No exceptions noted.

5.6 Taxation

Control Objective	Related Control	Frequency	Procedure	Results
E.17 Tax policy is updated and reviewed on a timely basis.	1. The tax treatment for significant corporate transactions is verified by internal tax advisors and an independent review of the myTax references is performed by the Company's Management and Taxation Accountant who works independently of the internal Wealth+ tax team.	Annually	Obtain the Corporate Actions register and ensure tax calculations are reviewed by the internal tax team. Ensure that the annual independent review of the myTax references is performed by the Management and Taxation Accountant.	No exceptions noted.

Control Objective	Related Control	Frequency	Procedure	Results
E.18 Tax information components and attributes used in the preparation of the income tax computation (current and deferred) are complete and calculated accurately in accordance with tax policy or as agreed with clients.	1. For each security held by Wealth+ clients the tax information components are entered from external tax statements. The Tax Stream leader verifies all that all tax components have been correctly entered into the Wealth+ system and evidences the check.	Annually	For a sample of securities inspect evidence of tax component check of the Tax Stream leader.	No exceptions noted.
	2. After generating the annual client reports, the Tax Team select a sample of reports and check accuracy and completeness prior to the reports being distributed to clients.	Annually	For a sample of annual client reports reviewed by the Tax Team inspect evidence of accuracy and completeness check.	No exceptions noted.

INFORMATION TECHNOLOGY CONTROL OBJECTIVES

SS&C appear to have strong IT controls that adequately meet the controls requirements of GS007. An unqualified opinion has been issued.

In determining the adequacy of SS&C's Wealth Platform IT controls as identified by GS007, Pitcher Partners relied upon the following independent auditors reports from PricewaterhouseCoopers Canada:

- SS&C Technology Canada Corporation. **Global Wealth Platform Application**: Report on the design of controls placed in operation and testing of operating effectiveness for the period October 1, 2021, to September 30, 2022. PricewaterhouseCoopers Canada 11 November 2022.
- SS&C Technology Canada Corporation. **(Data centres – Windsor, Connecticut ("CT"), Yorktown and Harrison, New York ("NY") as well as Mississauga, Ontario ("ON") Canada**: Report on the design of controls placed in operation and testing of operating effectiveness for the period October 1, 2021, to September 30, 2022. PricewaterhouseCoopers Canada 11 November 2022.

The exceptions to this being control objectives G.3 and G.10 whereby Pitcher Partners Brisbane performed additional testing to satisfy the control objective. These related controls have been noted in the report following and reference is made to Pitcher Partners where applicable.

Based on the information attained from our review of these two documents, additional testing performed by Pitcher Partners and through discussions with Morgans' management we have assessed the following GS007 IT controls as being adequate.

The Canadian and American Standards used to conduct the review of SS&C's Wealth Platform IT Controls differ in structure and breakdown from the Australia Standard document – GS007. Therefore to facilitate a clear mapping of relevant controls, the following table contains extracted text from the original PWC reports placed against the relevant GS007 section.

In addition to the formal controls, Morgans have a strong relationship with SS&C as a vendor and maintain close and frequent contact with them. Wealth+ service reliability and stability is high, with application support being reliably delivered, with Morgans able to participate and use SS&C's Global Wealth Platform UAT environment for their own testing.

5.7 Restricting access to systems and data

Control Objective	Related Control	Frequency	Procedure	Results
G.1 Physical access to computer networks, equipment, storage media and program documentation is restricted to authorised individuals.	<p>SS&C Technology Canada Corporation. Mississauga Data Centre: Report on the design of controls placed in operation and testing of operating effectiveness for the period October 1, 2021 to September 30, 2022. PricewaterhouseCoopers 2022.</p> <p>Control objective 2</p> <p>(2A) A computerized key card and/or biometric scan system controls access to the SS&C Mississauga data center to prevent unauthorized access.</p>	Daily or many times daily	Observed the SS&C Mississauga data center to determine whether a biometric scan and/or key card were required to access the data center.	No exceptions noted.
	(2B) New access to the SS&C Mississauga data center is approved by management before being granted.	Daily or many times daily	For a sample of users granted access to the SS&C Mississauga data center, inspected access requests to determine whether the access was authorized prior to being granted.	No exceptions noted
	(2C) Key card access is disabled upon employee termination by appropriate SS&C Information Technology Group, Administrative, or Human Resources personnel to prevent unauthorized access.	Daily or many times daily	For a sample of terminated users, inspected the data center access list to determine whether their access was removed or deactivated on a timely basis.	No exceptions noted
	(2D) Physical access to the SS&C Mississauga data center is restricted to designated personnel. There is a monthly review of physical access to the data center. Access modification is performed as required by department administrators, administrative, or Human Resources personnel.	Daily or many times daily	<p>For a sample of months, inspected monthly access reviews to determine whether access to the data center was reviewed and changes in access identified by the review were actioned.</p> <p>Reperformed the review for a sample of users to determine whether user access was restricted to appropriate personnel.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
	(2E) Monitoring of the SS&C Mississauga data center is performed by the Data Center Operations team. Video surveillance cameras are placed within the SS&C Mississauga data center and used in the case of a problem. Visitors who require access to the data centers are escorted by SS&C personnel after	Daily or many times daily	<p>Observed the SS&C Mississauga data center to determine whether the data center was monitored by the Data Center Operations team using video surveillance cameras placed within the data center.</p> <p>Observed the Mississauga data center to determine whether SS&C Data Center</p>	No exceptions noted.

Control Objective	Related Control	Frequency	Procedure	Results
	ascertaining the purpose of the visit to the data center.		personnel escorted visitors requiring access to the data center after ascertaining the purpose of the visit.	
G.2 Logical access to programs, data and computer resources is restricted to appropriate and authorized individuals.	<p>SS&C Technology Canada Corporation. Mississauga Data Centre: Report on the design of controls placed in operation and testing of operating effectiveness for the period October 1, 2021 to September 30, 2022. PricewaterhouseCoopers 2022.</p> <p>Control objective 1</p> <p>Operating Systems (Open VMS, Oracle® Solaris and Windows®)</p> <p>(1A) Notification of new users, including administrators, must be provided by management to authorise access to the corporate Active Directory domain, and is required prior to additional access to applications and data.</p> <p>A Private Cloud employee transfer ticket is automatically generated when an employee transfer event is detected. Private Cloud access is modified as requested.</p>	Daily or many times daily	<p>For a sample of new SS&C employees, inspected the Electronic Hire Notification forms to determine whether Active Directory access was authorised by the Human Resources Department prior to access being granted.</p> <p>For a sample of transferred employees during the period, inspected evidence to determine whether legacy access was removed, and any new access was authorized by their new reporting manager</p>	No exceptions noted.
	(1B) In the event of a notification by HR of an employee termination, the employee's SS&C corporate Active Directory accounts are removed or disabled to prevent unauthorised access.	Daily or many times daily	For a sample of terminated users, inspected Active Directory and the corresponding termination tickets to determine whether Active Directory accounts had been either removed or disabled timely.	No exceptions noted.
	(1C) Users granted privileged server access are reviewed on a quarterly basis by appropriate authority for access appropriateness.	Daily or many times daily	For a sample of quarterly database administrator reviews, inspected the review evidence to determine whether the database administrator access reviews were performed, and that any modifications were processed completely and accurately, if applicable. For a sample of users, reperformed Management's review to determine whether database administrator access was restricted to appropriate personnel.	No exceptions noted.

Control Objective	Related Control	Frequency	Procedure	Results
	(1D) Privileged O/S access is restricted to users with a corresponding approved request. Users are restricted from approving their own requests, and access is granted on a temporary basis..	Daily or many times daily	Observed a login attempt using credentials with no corresponding approved temporary break-glass access request to determine whether privileged O/S access is restricted to users with a corresponding approved temporary break-glass access request. Observed an initiating user attempt to self-approve a break-glass request to determine whether there is segregation of duties enforced preventing a request from being approved by the initiating user. Observed a request for breakglass credentials exceeding a 72-hour duration to determine access is provisioned on a temporary basis. For a sample of privileged O/S access granted during the period, inspected evidence to determine whether users who were granted privileged server O/S access were approved and provisioned on a temporary basis by management	No exceptions noted. No exceptions noted.
	(1E) Active Directory password controls (minimum length, expiration, history, and lockout threshold) are enforced based on the Information Security Policy.	Daily or many times daily	Inspected the Windows Active Directory password configurations to determine whether minimum length, expiration, history and lockout threshold were enabled for the Private Cloud, and enforced based on the Information Security Policy.	No exceptions noted.
	(1F) For servers managed by EMS on the Private Cloud Platform - Privileged O/S access is approved and provisioned on a temporary basis by Management.	Daily or many times daily	For a sample of break-glass access granted during the period, inspected evidence to determine whether users who were granted privileged server O/S access were approved and provisioned on a temporary basis by management.	No exceptions noted.
	SS&C Technology Canada Corporation. Global Wealth Platform Application: Report on the design of controls placed in operation and testing of operating effectiveness for the period October 1, 2021 to September 30, 2022. PricewaterhouseCoopers 2022.		Inquired of SS&C management to determine whether password configuration standards are in place, including, but not limited to minimum password length, complexity and password expiry period.	

Control Objective	Related Control	Frequency	Procedure	Results
	<p>Compliance Checks - GWP Model™, GWP Trade™ and GWP Portfolio™</p> <p>Control objective 1</p> <p>Application Logical Security - GWP Model™, GWP Trade™ and GWP Portfolio™</p> <p>(A4) Password configuration standards are in place, including, but not limited to, minimum password length, complexity and password expiry period.</p>	Daily or many times daily	<p>Inspected the system password configuration and determined settings exist for minimum password length, password expiry and complexity.</p> <p>Using a test account, observed user change their password to determine whether the system enforced the configuration setting established for that Business Unit.</p>	No exceptions noted.
	<p>(A5) User accounts are locked after a set number of invalid attempts, the sign-on session is terminated and the user ID is suspended.</p>	Daily or many times daily	<p>Inquired of SS&C management to determine whether user accounts are locked after a set number of invalid attempts, the sign-on session is terminated and the user ID is suspended requiring the user to contact the relevant client or SS&C administrator to reset the ID.</p> <p>Inspected the Business Unit configuration to determine whether user accounts are locked after a set number of invalid attempts.</p> <p>Using a test account, observed a user attempt to sign into the system to determine that once the user exceeded the defined number of invalid login attempts, the sign-on session was terminated and the user ID locked.</p>	No exceptions noted.
	<p>(A6) Access of SS&C personnel to corporate Active Directory is granted and modified based on management approval, and is revoked timely upon termination.</p>	Daily or many times daily	<p>Inquired of SS&C management to determine whether access of SS&C personnel to corporate AD is granted and modified based on management approval, and is revoked timely upon termination.</p> <p>For a sample of new users, inspected supporting documentation to determine whether access to corporate AD is granted based on management approval.</p> <p>For a sample of terminated users, inspected supporting</p>	No exceptions noted.

Control Objective	Related Control	Frequency	Procedure	Results
			<p>documentation to determine whether access to corporate AD is revoked timely.</p> <p>For a sample of terminated users, inspected supporting documentation to determine whether access to corporate AD is revoked timely.</p>	
	<p>(A7) Logical Access to the Active Directory for terminated users is reviewed on a monthly basis. Access modification is performed as required by department administrators, administrative or Human Resources personnel.</p>	<p>Daily or many times daily</p>	<p>Inquired of management to determine whether logical access to the Active Directory for terminated users is reviewed on a monthly basis and access is modified as required by department administrators, administrative or Human Resources personnel.</p> <p>For a sample of months, inspected monthly access reviews to determine whether access to the Active Directory was reviewed and changes in access identified by the review were actioned.</p> <p>Reperformed the review for a sample of users to determine whether user access was restricted to appropriate personnel.</p>	<p>No exceptions noted.</p>
	<p>Account Set up and Maintenance – GWP Model™, GWP Trade™ and GWP Portfolio™</p> <p>(A3) Clients are restricted to their assigned business unit and data through a combination of the universal system identifier (for their assigned business unit), user ID.</p> <p>Clients can use IP filtering to further restrict business unit access.</p>	<p>Daily or many times daily</p>	<p>Inquired of SS&C management to determine whether clients can only access their assigned business unit and data through a combination of the universal system identifier (for their assigned business unit), user ID and clients can use IP filtering to restrict business unit access.</p> <p>Inspected the LDAP (Lightweight Directory Access Protocol) directory tree and configuration settings for a sample of client business units on the production system to determine that they are set up as unique and logically separate units, and that client users are restricted to their assigned business units only.</p>	<p>No exceptions noted.</p>

Control Objective	Related Control	Frequency	Procedure	Results
			<p>Using a test account, observed the GWP logon process to determine that access to business units could only be obtained through a valid combination of universal system identifier and user ID.</p> <p>Using a test account, observed a user attempt to sign into a business unit from an IP address that is not in the defined "Whitelist" of addresses to determine whether they were prevented from doing so.</p>	
	<p>Application Logical Security – GWP Advisor™</p> <p>(B4) The application enforces password parameters configured within the system for each client.</p>	Daily or many times daily	<p>Inquired of SS&C management to determine whether the application enforces password parameters configured within the system for each client.</p> <p>Observed a user log onto the system and change their password and determined that system enforced the password policy established for the user's business unit.</p>	No exceptions noted.
	<p>(B5) Based on the client configuration setup, user accounts are locked after a set number of invalid attempts, the sign-on session is terminated and the user ID is suspended. The permissions necessary to unlock an operator ID are restricted to users granted access to those specific functions.</p>	Daily or many times daily	<p>Inquired of SS&C management to determine whether based on the client configuration setup, user accounts are locked after a set number of invalid attempts, the sign-on session is terminated and the user ID is suspended requiring the user to contact the relevant system administrators including SS&C administrators, SS&C business support staff or client users with administrator level privileges.</p> <p>Observed a user attempt to logon to the system to determine whether once the user exceeded the number of defined invalid login attempts, the sign-on session was terminated and the user ID was suspended.</p> <p>Observed a user log in using one account with the permission to unlock an operator ID and another</p>	No exceptions noted.

Control Objective	Related Control	Frequency	Procedure	Results
			account with no permission to unlock the operator ID to determine whether the permissions necessary to unlock an operator ID are restricted to users granted access to those specific functions.	
G.3 Segregation of incompatible duties is defined, implemented and enforced by logical security controls in accordance with job roles.	<p>SS&C Technology Canada Corporation. Global Wealth Platform Application: Report on the design of controls placed in operation and testing of operating effectiveness for the period October 1, 2021, to September 30, 2022. PricewaterhouseCoopers 2022.</p> <p>Control objective 1</p> <p>Account Set up and Maintenance – GWP Model™, GWP Trade™ and GWP Portfolio™</p> <p>(A1) Client business unit set up and maintenance of existing business units (if application) are performed in accordance with formal client instructions by designated SS&C personnel based on authorised service agreements.</p>	Daily or many times daily	<p>Inquired of SS&C management to determine whether client business unit setup and maintenance of existing business units were performed in accordance with formal client instructions by designated SS&C personnel based on authorised service agreements.</p> <p>For a sample of new client business units and changes made to existing client business units, inspected supporting documentation to determine whether the client business units were set up in accordance with formal client instructions by designated users based on an authorised service contract.</p> <p>For a sample of existing business units, inspected supporting documentation to determine whether the maintenance of existing client business units was performed in accordance with formal client instructions by designated SS&C personnel based on an authorised service contract.</p>	No exceptions noted.
	<p>Testing performed by Pitcher Partners, Brisbane.</p> <p>1. Segregation of duties has been designed in such a way to segregate key processes within Back Office operations. The key tasks that have been segregated include Account Maintenance (creation /</p>	Daily or many times daily	Obtain the user list for both the GWP and the Back Office operations and identify users who have access to both systems.	<p>No exceptions noted.</p> <p>No exceptions noted.</p>

Control Objective	Related Control	Frequency	Procedure	Results
	modifying of accounts) SCRIP (stock movement and corporate action processing) and Cash Accounts (control over Cash movements / Term Deposits). Wealth+ staff have minimal access to GBST Shares and only a small subset of staff can perform system updates based specifically on their role.		For identified users, review system permissions of the Back Office operations to ensure appropriate based on their job profile.	

5.8 Authorising and processing transactions

Control Objective	Related Control	Frequency	Procedure	Results
G.4 IT processing is authorised and scheduled appropriately and deviations are identified and resolved in a timely manner.	<p>SS&C Technology Canada Corporation. Global Wealth Platform Application: Report on the design of controls placed in operation and testing of operating effectiveness for the period October 1, 2021 to September 30, 2022. PricewaterhouseCoopers 2022.</p> <p>Control objective 2</p> <p>Contact and Account Access Controls – GWP Model™, GWP Trade™ and GWP Portfolio™</p> <p>(A1) Where access is controlled through the use of RR Codes, RR Codes are mandatory fields for Contacts and Accounts. The application prevents an account or contact from being created unless an RR Code is assigned.</p>	Daily or many times daily	<p>Inquired of SS&C management to determine whether the system prevents users from creating an account or contact unless an RR code is assigned to the user.</p> <p>Observed a user attempt to create an account and contact to determine whether they were not created unless an RR code was assigned to that account or contact</p>	No exceptions noted.
	(A2) Where the Business Unit is configured to control access through the use of RR Codes, the combination of RR code assigned to a user and RR code assigned to an account determines whether the user can access that account. The system user only permits a user	Daily or many times daily	Inquired of SS&C management to determine whether the system will allow a user to gain access to an account only if an RR code is assigned or if one of the RR codes assigned to the user matches the RR code assigned to the account.	No exceptions noted.

Control Objective	Related Control	Frequency	Procedure	Results
	to gain access to an account if either: <ul style="list-style-type: none"> A user has been assigned an RR Code of <i>Master RR</i>, or One of the RR Codes assigned to a user matches the RR Code assigned to a contact. 		Observed a user attempt to access an account to determine whether the user could access an account only if the User ID was assigned an RR code or a Master RR code and only if the RR code assigned to a user matched the RR Code assigned to the account.	
	<p>(A3) Where the Business Unit is configured to control access through the use of RR Codes, the combination of RR code assigned to a user and RR code assigned to a contact determines whether the user can access that contact. The system will only permit a user to gain access to a contact if either:</p> <ul style="list-style-type: none"> RR access code control is explicitly disabled for that user; The contact has been assigned an RR Code of <i>Global Access</i>; A user has been assigned an RR Code of <i>Master RR</i>; or One of the RR Codes assigned to a user matches the RR Code assigned to a contact. 	Daily or many times daily	<p>Inquired of SS&C management to determine whether the system restricts access to a contact based on the RR Code assigned to the user ID and the contact.</p> <p>For a sample of cases, observed a user attempt to access a contact to determine whether the system only permitted access if either:</p> <ul style="list-style-type: none"> RR access code control is explicitly disabled for that user; The contact has been assigned an RR Code of <i>Global Access</i>; A user has been assigned an RR Code of <i>Master RR</i>; or One of the RR Codes assigned to a user matches the RR Code assigned to a contact. 	No exceptions noted.
	<p>(A4) Where the Business Unit is configured to control access through the use of <i>Portfolio Data Access Sets</i>, the system only permits a user to access an account if both the User and Account have been assigned to the same Portfolio Data Access Set.</p>	Daily or many times daily.	<p>Inquired of SS&C management to determine whether the system only permits a user to access an account if both the user and account have been assigned to the same Portfolio Data Access Set.</p> <p>For a sample of cases, observed a user attempt to access an account to determine whether access was only permitted if both the user and account have been assigned to the same Portfolio Data Access Set.</p>	No exceptions noted.
	Account Approval Controls – GWP Model™, GWP Trade™ and GWP Portfolio™	Daily or many times daily	Inquired of SS&C management to determine whether the system enforces state approval. Specifically, the progression to a state is only permitted if the user ID has been assigned that	No exceptions noted.

Control Objective	Related Control	Frequency	Procedure	Results
	<p>(A5) Where a business unit has been configured to enforce states for accounts:</p> <ul style="list-style-type: none"> The system will only permit a user to approve an account for progression to a state, when that state has been assigned to that user. The account must be in an appropriate state (as defined by business unit static data). The static data for the state with flag, enable activation, establishes the first state that the account may be activated. The account may also be activated at any subsequent state. The system gives a user the ability to lock the documentation. While in a locked state, documentation cannot be modified or deleted. 		<p>state; and that an account can only be activated when the user ID has been assigned the appropriate state.</p> <p>For a sample of cases, observed a user attempt to progress an account to determine whether they could only do so if their user ID had been assigned the state to which they were attempting to progress the account.</p> <p>Observed a user attempt to activate an account in a sample of account states to determine if the account state can only be activated if that account state has been enabled.</p> <p>Observed a user attempt to delete a file that had been locked by a user with 'Protect Contact Account Documentation' privilege to determine whether the system prevented the file from being deleted.</p>	
	<p>Control objective 3</p> <p>Input and Processing Checks - GWP Model™, GWP Trade™ and Portfolio™</p> <p>(A1) The system only allows users to process transactions based on their assigned permissions.</p> <ul style="list-style-type: none"> Only an appropriately permissioned user can access trading modules. Only users assigned to a desk can see the orders assigned to that desk. A user must claim an order before they are able to trade it; no other user can subsequently claim that order. Orders with compliance breaches cannot be released to a desk and can only be authorised by specific users. 	Daily or many times daily	<p>Inquired of SS&C management to determine whether the system only allows users to process transactions based on their assigned permissions.</p> <p>Using a test account, observed a user process a sample of transactions to determine whether the system only allowed the user to process transactions based on their assigned permissions.</p> <p>Only an appropriately permissioned user can access trading modules.</p> <p>Only users assigned to a desk can see the orders assigned to that desk.</p> <p>A user must claim an order before they are able to trade it; no other user can</p>	No exceptions noted.

Control Objective	Related Control	Frequency	Procedure	Results
			subsequently claim that order. Orders with compliance breaches cannot be released to a desk and can only be authorized by specific users.	
	<p>(A4) GWP Trade™ and GWP Model™ have a user defined security price limit check which is executed by the system before an order is placed. An exception message is generated in case of any price deviation for client notification and correction.</p> <p>Changes to security price limit parameter can be made by users who have been granted access to that function (such as users with the default compliance officer role). Changes are tracked in the audit trail.</p>	Daily or many times daily	<p>Inquired of SS&C management to determine whether the GWP trade and GWP model have a user defined security price limit check which is executed by the system every time an order is placed, and an exception message is generated for client notification and correction anytime the deviation exceeds the defined limits. Also inquired to determine whether changes to the security price limit parameters can be made by client designated users (e.g. compliance officer) only.</p> <p>Using a test account, observed a user enter trades to determine whether the system generated exception messages when the price entered exceed the defined price deviation thresholds.</p> <p>Using a test account, observed a user attempt to modify the price limit thresholds to determine whether access was denied if the user ID did not have that level of access.</p>	No exceptions noted
	<p>(A5) GWP Portfolio™ and GWP Model™ assign unique and sequential reference numbers to transactions so that they can be identified and traced easily throughout the processing cycle.</p>	Daily or many times daily	<p>Inquired of SS&C management to determine whether GWP Portfolio™ and GWP Model™ assign unique and sequential reference numbers to transactions so that transactions can be identified and traced easily throughout the processing cycle.</p> <p>Observed a user create a transaction to determine whether transactions were assigned unique and sequential reference numbers.</p>	No exceptions noted.

Control Objective	Related Control	Frequency	Procedure	Results
	(A6) Cancelled / corrected trades are automatically flagged by the system and a history of these changes is recorded and can be retrieved for audit purposes.	Daily or many times daily	<p>Inquired of SS&C management to determine whether the system automatically flags cancelled or corrected trades and that a history of these changes can be retrieved for audit purposes.</p> <p>Using a test account, observed a user:</p> <ul style="list-style-type: none"> Cancel a trade and inspected the transaction history report to determine whether the system automatically flagged the trade as cancelled. Modify a trade, inspected the transaction history to determine whether the system marked the trade as modified. 	No exceptions noted.
	(A7) For modified transactions, a new record is created for each version of the transaction. Details of these transactions are available for audit purposes. These details include the user ID and date/timestamp of the system override.	Daily or many times daily	<p>Inquired of SS&C management to determine whether the system creates a new trade record for every version of a modified trade, including the user ID and date/timestamp of the system override.</p> <p>Using a test account, observed the processing of a modified trade and inspected the transaction history reports to determine whether the system maintains a log of the trades history including user ID and date/timestamp of the modification.</p>	No exceptions noted.
	(A8) The system only permits trades to be processed in GWP Portfolio™ with pre-defined counterparties, as defined by clients	Daily or many times daily	<p>Inquired of SS&C management to determine whether trades can only be processed in GWP Portfolio with predefined counterparties as defined by clients</p> <p>Using a test account, for a selection of cases, observed a user enter a trade in GWP Portfolio to determine whether counterparties could only be selected from a list of predefined counterparties.</p>	No exceptions noted.
	(A9) The system can be configured to allow for the	Daily or many times daily	Inquired of SS&C management to determine whether corporate action	No exceptions noted.

Control Objective	Related Control	Frequency	Procedure	Results
	<p>automatic application of corporate action information. Activities received after their expected process date are flagged as suspended. Suspended activities require further review and acceptance by appropriate personnel before processing can take place. Users that do not have permission to maintain securities cannot modify the corporate action details.</p>		<p>notifications received from external sources (e.g. Bloomberg/the custodian) are applied automatically.</p> <p>Using a test account, observed the processing of corporate action to determine whether corporate actions were automatically applied.</p> <p>Using a test account, observed whether activities received after their expected process date are flagged as suspended, and whether suspended activities require further review and acceptance before processing can take place.</p> <p>Using a test account, for a sample of cases, observed a user attempt to manually modify corporate action and determined that only a user with "maintain security privilege" could do so.</p>	
	<p>(A10) Compliance rules (either flexible or firm) can only be set up by users who have been granted access to that function.</p> <p>Any amendment to or overriding of the compliance rules is logged in the system. Flexible constraints can be overridden by users with the appropriate permission level</p>	Daily or many times daily	<p>Inquired of SS&C management to determine whether compliance rules can be set up by designed users only and that any amendment to or overriding of the compliance rules in logged in the system.</p> <p>Using a test account, for a selection of scenarios, observed a user attempt to set up and amend compliance rules to determine whether access was denied if the user ID had not been granted that level of access</p> <p>Using a test account, observed a user override a compliance rule to determine whether the override was logged in the system.</p>	No exceptions noted.
	<p>(A11) Pre-trade, on create and passive compliance checks are performed by the system based on pre-defined compliance rules as set up by client users. Any exceptions are recorded in the activity log for client</p>	Daily or many times daily	<p>Inquired of SS&C management to determine whether pre-trade, on-create and passive compliance checks are performed by the system based on predefined compliance rules as set up</p>	No exceptions noted.

Control Objective	Related Control	Frequency	Procedure	Results
	investigation and resolution purposes.		<p>by client users, and that any exceptions are recorded in the activity log for the client investigation and resolution purposes.</p> <p>Using a test account, observed a user process trade for a selection of cases to determine whether compliance exceptions were recorded in the activity log.</p> <p>Using a test account, observed a user run a passive compliance job to determine whether compliance exceptions were recorded in the activity log.</p>	
	<p>Reporting – GWP Model™, GWP Trade™, GWP Portfolio™ and GWP Advisor™</p> <p>(A12) Client users are restricted to running and viewing the default reports based on their privileges. Access to reporting parameters is restricted to client users who have been granted access to that function.</p>	Daily or many times daily	<p>Inquired of SS&C management to determine whether client users are restricted to running and viewing the default reports based on their privileges and that access to reporting parameters is restricted to authorised client users only.</p> <p>Using a test account, for a selection of scenarios, observed a user attempt to access reports to determine whether access was denied if the user ID has not been granted that level of access.</p>	No exceptions noted.
	<p>(A13) Exception Reports can be generated from the compliance monitoring system based on a pre-defined frequency and rules, as set up by client users, listing accounts that exceed asset mix or permitted security constraints.</p> <p><i>(Not applicable to GWP Advisor™)</i></p>	Daily or many times daily	<p>Inquired of SS&C management to determine whether compliance exception reports can be generated from the compliance monitoring system based on a pre-defined frequency as set up client users, listing accounts that exceed asset mix or permitted security constraints.</p> <p>Using a test account, observed a user define compliance reporting to determine whether the reporting frequency and</p>	No exceptions noted.

Control Objective	Related Control	Frequency	Procedure	Results
			<p>rules to be reported could be specified.</p> <p>Inspected the compliance Exception Report to determine whether it includes the results of the compliance checks.</p>	
	<p>Logging – GWP Model™, GWP Trade™, GWP Portfolio™ and GWP Advisor™</p> <p>(A14) All transactions and client user activities are logged by the system with date, time and operator ID.</p>	Daily or many times daily	<p>Inquired of SS&C management to determine whether all transactions and client user activities are logged by the system with date, time and operator ID for retention and investigation by clients.</p> <p>Inspected the log resulting from processing a selection of transactions using a test account and noted that the log maintained a record of those transactions including details of the Operator ID, date/time stamp and activity performed.</p>	No exceptions noted.
	<p>Other Transaction Processing Controls – GWP Model™, GWP Trade™, GWP Portfolio™ and GWP Advisor™</p> <p>(A15) Rebalance profiles</p> <p>Where the current weight of the individual sub portfolio has deviated more than the predefined drift threshold, the master model rebalance functionality generates orders to bring the related sub portfolios back in line with the specified weight constraints.</p>	Daily or many times daily	<p>Inquired of SS&C management to determine whether the rebalance functionality is in place to monitor that related sub portfolios adhere to predetermined weight constraints provided that the current weight of the individual sub-portfolio has deviated more than the predefined drift threshold.</p> <p>Using a test account, observed a user run the master model rebalance function to determine whether the application generated orders to bring the portfolio back in line with the specified weight constraints.</p>	No exceptions noted.
	<p>(A16) Order Netting (Stage 1)</p> <p>For stage 1 netting, the system will only net buy and sell orders when all the orders are:</p> <ul style="list-style-type: none"> • For the same security • Of the same multi strategy portfolio; and 	Daily or many times daily	<p>Inquired of SS&C management to determine whether for Stage 1 Netting, the system requires that the orders must be:</p> <ul style="list-style-type: none"> • for the same security of the same client; and • of the same account type. 	No exceptions noted.

Control Objective	Related Control	Frequency	Procedure	Results
	<ul style="list-style-type: none"> Of the same account type 		<p>Using a test account, observed a user use the stage 1 Netting functionality to determine whether only orders that met the following netting criteria were netted:</p> <ul style="list-style-type: none"> for the same security; of the same portfolio; and of the same account type. 	
	<p>(A17) Header and Trailers – import files</p> <p>Where the option to check header and trailer records is activated, files imported into their system are automatically verified for integrity and completeness based on the header and trailer record in the files. Batch numbers are created for imports and kept in audit logs (searchable by specific dates and actions) in the user interface.</p>	Daily or many times daily	<p>Inquired of SS&C management to determine whether files imported into the system are automatically verified for integrity and completeness.</p> <p>Using a test account, for a selection of cases, observed a user import files to determine whether files imported into the system were automatically verified for integrity and completeness based on the header/trailer records.</p>	No exceptions noted.
	<p>(A18) Headers and Trailers – Export Files</p> <p>If selected by the user, the system automatically creates a unique stamp in the header and/or trailer of an exported file to assist in verifying the integrity and completeness of the transactions exported.</p>	Daily or many times daily	<p>Inquired of SS&C management to determine whether the system automatically creates a unique stamp in the header and/or trailer of an export file to assist in verifying the integrity and completeness of the transactions exported, if selected by the user.</p> <p>Using a test account, observed a user export a file of transactions to determine whether the system automatically created a unique stamp in the header and/or trailer of the exported file.</p>	No exceptions noted.
	<p>(A19) Dynamic Security Models</p> <p>When the 'Dynamic Weights Update' task is run for security models designated as 'dynamic', the system automatically updates the asset allocation weights for individual securities, based on changes in market prices and foreign exchange rates from the effective date of the model to the current 'as of' date of the execution task.</p>	Daily or many times daily	<p>Inquired of SS&C management to determine whether the security models designated as 'dynamic', the 'Dynamic Weights Update' task are run automatically to update the asset allocation weights for individual securities, based on changes in market prices and foreign exchange rates.</p>	No exceptions noted.

Control Objective	Related Control	Frequency	Procedure	Results
			Using a test account, observed a user run the 'Dynamic Weights update' task to determine whether the asset allocation weights for individual securities automatically changed as market prices and foreign exchange rates fluctuate.	
	<p>(A20) Unitised Funds</p> <p>For unitised products, the system allows entry of value-based orders. For these orders the number of units is calculated accurately based on the net-asset-value (price) of the fund.</p>	Daily or many times daily	<p>Inquired of SS&C management to determine whether the system allows entry of value-based orders for unitised products and calculates the number of units accurately based on the net-asset-value (price) of the fund.</p> <p>Using a test account, observed a user enter an unitised fund order as 'Value' orders to determine whether the system accepted the order and automatically calculated the equivalent number of units based on net asset value.</p> <p>Re-performed the calculation to determine whether the system accurately calculated of the number of units based on the net-asset-value (price) of the fund.</p>	No exceptions noted.

5.9 Safeguarding assets

Control Objective	Related Control	Frequency	Procedure	Results
G.5 Appropriate measures, including firewalls and anti-virus software, are implemented to counter the threat from malicious electronic attack.	SS&C Technology Canada Corporation. Mississauga Data Centre: Report on the design of controls placed in operation and testing of operating effectiveness for the period October 1, 2021 to September 30, 2022. PricewaterhouseCoopers 2022. Control objective 5 (5A) For the Mississauga Data Center – Dedicated firewalls exist which have predefined rules for allowing in-bound and outbound traffic	Daily or many times daily	For a sample of connection types, inspected the firewall rules to determine whether rules were set up with pre-defined rules to restrict in-bound and out-bound traffic.	No exceptions noted.
	(5B) For the Mississauga Data Center – A network vulnerability test is performed to assess the security and vulnerabilities of applications on a quarterly basis. Management is notified of security issues (if any) for review and resolution.	Daily or many times daily	For a sample of quarters, inspected vulnerability reports to determine whether network testing was performed, vulnerabilities were assessed, and that management was notified of security issues for review and resolution.	No exceptions noted.
G.6 The physical IT equipment is maintained in a controlled environment.	SS&C Technology Canada Corporation. Mississauga Data Centre: Report on the design of controls placed in operation and testing of operating effectiveness for the period October 1, 2021 to September 30, 2022. PricewaterhouseCoopers 2022. Control objective 2 (2A) Physical access to data centers is managed through a key card and/or biometric scan to prevent unauthorized access.	Daily or many times daily	Observed a SS&C data center entrance point to determine whether a biometric scan and/or key card was required to access the data centers	No exceptions noted.
	(2B) Physical access to the Data Centers requires Management approval prior to access being provisioned	Daily or many times daily	GlopecOp, Windsor, Winchester Bridgeton, and Mississauga Data Centers For a sample of users granted access to the SS&C data centers, inspected key card authorizations to test whether access was authorized by management prior to access being granted.	No exceptions noted.

Control Objective	Related Control	Frequency	Procedure	Results
	(2C) Physical access to the Data Centers is revoked after notification of employee termination to prevent unauthorized access.	Daily or many times daily	GlopeOp, Windsor, Winchester Bridgeton, and Mississauga Data Centers For a sample of terminated users, inspected termination tickets and data center access lists to determine whether access was disabled in a timely manner.	No exceptions noted.
	(2D) Management performs reviews to ensure that physical access to the Data Centers is restricted appropriately.	Daily or many times daily	GlopeOp, Windsor, Winchester and Bridgeton Data Centers For the annual recertification, inspected evidence to determine whether the recertification of data center access was performed, and modifications were performed as requested. Reperformed the review for a sample of users to determine whether user access was restricted to appropriate personnel. Mississauga Data Center For a sample of months, inspected monthly access reviews to determine whether access to the data center was reviewed and changes in access identified by the review were actioned. Reperformed the review for a sample of users to determine whether user access was restricted to appropriate personnel.	No exceptions noted.
	(2E) Physical security management records access to data centre and computer room entry points. Security personnel monitor and respond to unauthorized activity at data centres and computer rooms	Daily or many times daily	GlopeOp, Windsor, Winchester Bridgeton, and Mississauga Data Centers Observed the SS&C data centres to determine whether the data centre was monitored by the Data Centre Operations team using video surveillance cameras placed within the data centre. Observed the SS&C data centres to determine whether SS&C personnel escorted visitors requiring access to the data centre after ascertaining the purpose of the visit.	No exceptions noted.

5.10

Maintaining and developing systems hardware and software

Control Objective	Related Control	Frequency	Procedure	Results
G.7 Development and implementation of new systems,	SS&C Technology Canada Corporation. Global Wealth Platform Application: Report		Inquired of SS&C management to determine	

Control Objective	Related Control	Frequency	Procedure	Results
applications and software, and changes to existing systems, applications and software, are authorised, tested, approved, implemented and documented.	<p>on the design of controls placed in operation and testing of operating effectiveness for the period October 1, 2021 to September 30, 2022. PricewaterhouseCoopers 2022.</p> <p>Control objective 4</p> <p>(A1) Changes to GWP (including new developments, codes, functionality enhancements, bug fixes, routine maintenance and emergency changes) are requested and approved prior to deployment.</p>	Daily or many times daily	<p>whether changes to GWP (including new developments, codes, functionality enhancements, bug fixes, routine maintenance and emergency changes) are requested and approved prior to development.</p> <p>For a sample of changes, inspected change documentation to determine whether the changes were requested and approved prior to deployment.</p>	No exceptions noted.
	(A2) Development and test/QA environments are segregated from the production environment.	Daily or many times daily	<p>Inquired of SS&C management to determine whether development and test/QA environments are segregated from the production environment.</p> <p>Observed the development, test/AQ and production environments to determine whether the development and test/QA environments were segregated from the production environment.</p>	No exceptions noted.
	(A3) Only designated SS&C support personnel are able to access application source code through the use of a version control utility system or Team Foundation Server (TFS).	Daily or many times daily	<p>Inquired of SS&C management to determine whether only designated SS&C support personnel are able to access application source code through the use of a version control utility system.</p> <p>Inspected the access list of the version control system (VCS) to determine whether access to the VCS tool was appropriate based on job responsibilities.</p>	No exceptions noted.
	(A4) In addition to any testing performed by the developer, independent testing is performed under the direction of the QA function in the test environment. QA provide sign-off of testing before the change request is submitted for approval.	Daily or many times daily	Inquired of SS&C management to determine whether in addition to any testing performed by the developer, independent testing is performed under the direction of the QA function in the test environment and QA provide sign-off of testing before the change request is submitted for approval.	No exceptions noted.

Control Objective	Related Control	Frequency	Procedure	Results
			For a sample of changes, inspected change documentation to determine whether QA provide sign-off of testing before the change request is submitted for approval.	
	(A5) Designated personnel test changes in a segregated testing environment. User acceptance testing approval/sign off are provided by management prior to implementation of changes in the production environment.	Daily or many times daily	<p>Inquired of SS&C management to determine whether designated personnel test changes in a segregated testing environment and that user acceptance testing approvals/sign offs are provided by management prior to implementation of changes in the production environment.</p> <p>For a sample of changes, inspected change documentation to determine whether user acceptance testing was performed and approvals/sign offs are provided prior to implementation of changes in the production environment.</p>	No exceptions noted.
	(A6) Changes are migrated to the production environment based on formal SS&C management approvals by a group who is independent of the developers.	Daily or many times daily	<p>Inquired of SS&C management to determine whether changes are migrated to the production environment based on SRB approval by a group who is independent of the developers.</p> <p>For a sample of changes, inspected change documentation to determine whether these changes were approved by the SRB prior to be being promoted to production by the Information Technology Services ("ITS") group (independent of the developers).</p>	No exceptions noted.
	(A7) Final and approved changes are documented in a functional specifications document prior to being released to the production environment.	Daily or many times daily	Inquired of SS&C management to determine whether all final and approved changes are documented in a functional specifications document prior to being released to the production environment.	No exceptions noted.

Control Objective	Related Control	Frequency	Procedure	Results
			For a sample of changes, inspected change documentation to determine whether a functional specifications document had been prepared prior to being released to the production environment.	
	<p>(A8) privileged access to operating systems is restricted to designed IT personnel. An annual review of operating administration access is performed. Access modification is performed as required by department administrators.</p> <p>Data Centre Operations ("DCO") grants a pre-approved developer temporary access to production based on a documented request specifying the reason access is required. DCO revokes the access on a timely basis unless an extension is requested.</p>	Daily or many times daily	<p>Inquired of SS&C management to determine whether an annual review of operating administration access is performed and access modification is performed as required by department administrators and whether the ability to migrate changes to production is restricted to authorised personnel and DCO revokes the access in a timely manner unless an extension is requested.</p> <p>For the annual privileged access recertification, inspected evidence to determine whether the recertification of OS administrators access was performed and modifications were implemented as requested.</p> <p>For a sample of developer access events to production, inspected documentation to determine whether access was granted based on a documented request and the access was revoked timely unless an extension request was provided.</p>	No exceptions noted.
G.8 Data migration or modification is authorised, tested and, once performed, reconciled back to the source data.	<p>SS&C Technology Canada Corporation. Global Wealth Platform Application: Report on the design of controls placed in operation and testing of operating effectiveness for the period October 1, 2021 to September 30, 2022. PricewaterhouseCoopers 2022.</p> <p>Control objective 3</p>		<p>Inquired of SS&C management to determine whether input trade data must pass clear predefined data edit and validation checks before the system accepts a trade for processing.</p> <p>Using a test account, for a selection of scenarios,</p>	

Control Objective	Related Control	Frequency	Procedure	Results
	Input and Processing Checks - GWP Model™, GWP Trade™ and Portfolio™ (A2) Input trade data must clear predefined edit and validation checks before the system accepts a trade for processing. Key edit and validation checks include: <ul style="list-style-type: none"> • Security identifier check (i.e. can only place an order for the security requested on the ticket) • Valid broker or counterparty code check • Order value and trade quantity checks (i.e. cannot place more shares than were ordered) • Price check (any changes to the price is captured in the audit trail) • Date checks (place date, fill date, settlement date, limit date) 	Daily or many times daily	observed a user enter trades to determine whether the below key edit and validation checks performed by the system were existing: <ul style="list-style-type: none"> • Security identifier check (i.e. can only place an order for the security that is known by the system) required on the ticket; • Valid broker or counterparty code check; • Order value and trade quantity checks (i.e. cannot place more shares than were ordered); • Price check (any changes to the price is captured in the audit trail); and • Date checks (place date, fill date, settlement date, limit date). 	No exceptions noted.
	(A3) Mandatory fields are required to be completed before a trade can be processed by the system. Key mandatory fields include: <ul style="list-style-type: none"> • Security identifier field; • Broker or counterparty code fields; • Trade quantity and price fields; • Currency fields; • Date and time fields. 	Daily or many times daily	Inquired of SS&C management to determine whether mandatory fields are required to be completed before a transaction can be processed by the system. Using a test account, observed a user enter trades to determine whether the system processes transactions only when below the key mandatory fields are completed. <ul style="list-style-type: none"> • Security identifier field; • Broker or counterparty code fields; • Trade quantity and price fields; • Currency field; and • Date and time fields. 	No exceptions noted.

5.11 Recovering from processing interruptions

Control Objective	Related Control	Frequency	Procedure	Results
G.9 Data and systems are backed up regularly	SS&C Technology Canada Corporation. Mississauga Data Centre: Report on the design of			

Control Objective	Related Control	Frequency	Procedure	Results
offsite and tested for recoverability on a periodic basis.	controls placed in operation and testing of operating effectiveness for the period October 1, 2021, to September 30, 2022. PricewaterhouseCoopers 2022. Control objective 3 (3A) Backups are performed based on system-configured schedules, where appropriate.	Daily or many times daily	GlopeOp Data Center For a sample of in-scope productions systems, inspected the master backup schedule to determine whether production systems are backed up periodically. Windsor Data Center For a sample of in-scope application servers and databases, inspected the master backup schedule to determine whether they are backed up regularly. Mississauga Data Center For a sample of in-scope production application and database servers, inspected the master backup schedule to validate that the servers were included in the daily and weekly backup schedules.	No exceptions noted.
	(3B) Notifications are provided to management for research and resolution when backups do not complete successfully.	Daily or many times daily	GlopeOp Data Center For a sample of in-scope production systems and days, inspected evidence of the daily report to determine whether backups for the in-scope productions systems ran successfully. For instances contained within our initial sample, where the backup failed, inspected evidence to validate resolution. Windsor and Mississauga Data Centers For a sample of automated backup failure email alerts, inspected evidence of follow-ups to determine whether backup failures that have occurred were identified, researched and resolved.	No exceptions noted.
	(3C) Backups are rotated, as appropriate, to off-site storage locations periodically, and logs are kept for each transfer.	Daily or many times daily	GlopeOp, Windsor, and Mississauga Data Centers For a sample of backup rotations, inspected evidence to determine whether backups were sent offsite.	No exceptions noted.
	(3D) Backup restoration procedures for critical systems are performed periodically to evaluate the integrity of data backups.	Daily or many times daily	GlopeOp, Windsor, and Mississauga Data Centers For a sample of restorations, inspected evidence for the backup restoration to determine whether the backup was restored successfully.	No exceptions noted.

Control Objective	Related Control	Frequency	Procedure	Results
	(3E) The SS&C Mississauga data center is equipped with an environmental monitoring system that is configured to notify SS&C personnel when predefined thresholds are exceeded	Daily or many times daily	Observed the SS&C Mississauga Data Center Operations personnel to determine whether a monitoring system was in place to notify SS&C personnel when predefined thresholds are exceeded.	No exceptions noted.
	(3F) The following environmental controls apply to the SS&C Mississauga data center: <ul style="list-style-type: none"> • Fire suppression and fire extinguishers • Multiple AC units • Water detection devices • Raised floors • Multiple uninterruptible power supply (UPS) systems Generator in place to support load in data center	Daily or many times daily	Observed the SS&C Mississauga data center to determine whether the following environmental controls existed: <ul style="list-style-type: none"> • Fire suppression and fire extinguishers • Multiple AC units • Water detection devices • Raised floors • Multiple uninterruptible power supply (UPS) systems Generator in place to support load in data center	No exceptions noted.
	(3G) The following infrastructure support systems are present at the SS&C Mississauga data center. Maintenance of these systems is carried out periodically: <ul style="list-style-type: none"> • Temperature control system • Humidity control system • Fire notification and suppression system • Uninterruptible Power Supply (UPS) system with generator support 	Daily or many times daily	For a sample of maintenance periods, inspected the periodic maintenance log for the temperature control system to determine whether the maintenance/test was successfully performed. For a sample of maintenance periods, inspected the periodic maintenance log for the humidity control system to determine whether the maintenance/test was successfully performed. For a sample of maintenance periods, inspected the periodic maintenance log for the fire notification and suppression system to determine whether the maintenance/test was successfully performed. For a sample of maintenance periods, inspected the maintenance log for the UPS system and generator support for a sample of maintenance periods to determine whether the maintenance/test was performed successfully.	No exceptions noted. No exceptions noted. No exceptions noted. No exceptions noted.

Control Objective	Related Control	Frequency	Procedure	Results
	Control objective 4 (4A) Changes to SS&C data center infrastructure, databases, and operating systems are authorized, tested as needed, approved and documented prior to implementation	Daily or many times daily	GlopeOp, Windsor, and Mississauga Data Centers For a sample of changes to infrastructure, databases, and operating systems, inspected the change tickets to validate that changes are authorized, tested as needed, approved and documented prior to implementation.	No exceptions noted.
	(4B) Emergency changes are implemented into production as required and are documented using standard change tickets and reviewed within 24 hours		For a sample of emergency changes inspected change tickets to validate that the emergency changes were reviewed by the relevant application owners within 24 hours of implementation of the change.	No exceptions noted.
	(4C) For servers managed by EMS on the Private Cloud Platform - Changes to infrastructure, databases, and operating systems are authorized and are approved prior to implementation.		For a sample of changes to infrastructure, databases, and operating systems, inspected the change documentation to determine whether changes were authorized and approved prior to implementation.	No exceptions noted.
	(4D) For servers managed by EMS on the Private Cloud Platform - Changes to infrastructure, databases, and operating systems are tested prior to implementation.		For a sample of changes to infrastructure, databases, and operating systems, inspected the change documentation to determine whether changes were tested prior to implementation.	No exceptions noted.
	(4E) For Private Cloud Servers managed by EMS - Changes to network Access Control Lists (ACL) are documented and approved by appropriate personnel prior to modification.		For a sample of network ACL changes, inspected evidence to determine whether the changes were approved by appropriate personnel appropriate personnel prior to modification.	No exceptions noted.
G.10 IT hardware and software issues are monitored and resolved in a timely manner.	Testing performed by Pitcher Partners, Brisbane. 1. Key systems jobs within GWP are configured to run on a defined schedule.	Daily or many times daily	Obtain the audit log of key system jobs run in the audit period and review to ensure the key system jobs are run at their required frequency.	No exceptions noted.
	2. An audit log is retained and stored for each system job that has been run.	Daily or many times daily	Sight audit log of key system jobs.	No exceptions noted.

Control Objective	Related Control	Frequency	Procedure	Results
	3. Monitoring of key system jobs is performed on an exceptions basis. Key system jobs are configured so that any jobs which are unsuccessful result in an email being sent to a Morgans IT mailbox informing them that the job failed.	Daily or many times daily	For a sample of key system jobs that failed or were incomplete, sight automated email sent to the Morgans IT mailbox.	No exceptions noted.
	4. Job failure emails are reviewed by IT personnel who will determine the appropriate course of action.	Daily or many times daily	For a sample of automated job failure emails sent to Morgans IT mailbox, sight evidence of follow up by IT personnel and ensure remediation of the exception was on a timely basis.	No exceptions noted.
	5. Any changes to scheduled system jobs are approved and tested within a User Acceptance Testing ("UAT") environment prior to final approval and promotion to the production environment.	Daily or many times daily	Obtain the audit log of scheduled system jobs with tasks for the first and last day in the audit period, review for any changes to these scheduled jobs. For changes identified, ensure approved and tested within a UAT environment prior to final approval and promotion to the production environment.	No exceptions noted.
G.11 Business and information systems recovery plans are documented, approved, tested and maintained.	<p>SS&C Technology Canada Corporation. Mississauga Data Centre: Report on the design of controls placed in operation and testing of operating effectiveness for the period October 1, 2021, to September 30, 2022. PricewaterhouseCoopers 2022.</p> <p>Control objective 3</p> <p>(3B) Backup failures are alerted on an ongoing basis by the backup systems. Failed backups are investigated and appropriate action is taken.</p>	Daily or many times daily	For a sample of automated backup failure email alerts, inspected evidence of follow-ups to determine whether backup failures that have occurred were identified, researched and resolved.	No exceptions noted.

5.12 Monitoring compliance

Control Objective	Related Control	Frequency	Procedure	Results
<p>G.12 Information technology services provided to clients are approved, managed and performance thresholds met in accordance with the requirements of the client agreement.</p>	<p>SS&C Technology Canada Corporation. Global Wealth Platform Application: Report on the design of controls placed in operation and testing of operating effectiveness for the period October 1, 2021, to September 30, 2022. PricewaterhouseCoopers 2022.</p> <p>Control objective 1</p> <p>Account Set up and Maintenance - GWP Model™, GWP Trade™ and GWP Portfolio™</p> <p>(A1) Client business unit set up and maintenance of existing business units are performed in accordance with formal client instructions by designated SS&C personnel based on authorised service agreements.</p>	Annually	<p>Inquired of SS&C management to determine whether client business unit set-up and maintenance of existing business units were performed in accordance with formal client instructions by designated SS&C personnel based on authorised service agreements.</p> <p>For a sample of new client business units and changes made to the existing client business units, inspected supporting documentation to determine whether the client business units were set up in accordance with formal client instructions by designated users based on an authorised service contract.</p> <p>For a sample of existing business units, inspected supporting documentation to determine whether the maintenance of existing client business units was performed in accordance with formal client instructions by designated SS&C personnel based on an authorised service contract.</p>	No exceptions noted.
	<p>(A2) Operational data (countries, currencies, exchanges and conventions), data sources (price, FX and risk sources) and network adapters are set up at the time of system implementation by designated</p>	Annually	<p>Inquired of SS&C management to determine whether operational data, data sources, and network adapters are set up by designated SS&C staff during the system implementation process</p>	No exceptions noted.

Control Objective	Related Control	Frequency	Procedure	Results
	SS&C staff based on approved client requirements.		<p>based on approved client requirements.</p> <p>For a sample of new clients set up, inspected supporting documentation to determine whether operational data, data sources, and network adapters were set up by designated users during the system implementation process based on approved client requirements.</p>	
	<p>Account Set up and Maintenance - GWP Advisor™</p> <p>(B1) Client website setup and maintenance of existing websites are performed in accordance with formal client instructions, by designated SS&C personnel and based on authorised service agreements.</p>	Annually	<p>Inquired of SS&C management to determine whether client website setup and maintenance of existing websites are performed in accordance with formal client instructions, by designated SS&C personnel and based on authorised service agreements.</p> <p>For a sample of new client websites, inspected supporting documentation to determine whether the client websites were set up in accordance with formal client instructions, by designated SS&C personnel and based on authorised service agreements.</p> <p>For a sample of existing websites, inspected supporting documentation to determine whether maintenance of existing websites was performed in accordance with formal client instructions by designated SS&C personnel and based on authorised service agreements.</p>	No exceptions noted.
	(B2) Client Entity Structures are set up at the time of system implementation by designated SS&C staff based on approved client requirements.	Annually	<p>Inquired of SS&C management to determine whether Client Entity Structures are set up at the time of system implementation by designated SS&C staff based on approved client requirements.</p> <p>For a sample of new clients set up, inspected supporting</p>	No exceptions noted.

Control Objective	Related Control	Frequency	Procedure	Results
			documentation to determine whether Client Entity Structures were set up at the time of system implementation: <ul style="list-style-type: none"> by designated SS&C staff; and based on approved client requirements. 	
	(B3) Clients are restricted to their assigned website and data through a combination of unique website address (URL), user name and password. Access to Modules is permission based so that users can only access the specific areas of the application to which they have been granted access.	Daily or many times daily	Inquired of SS&C management to determine whether clients can only access their assigned website and data through a combination of the unique website address, user name and password. For a sample of clients, inspected the configuration settings for the client websites to determine whether they were set up as unique and logically separate websites, and that client users are restricted to their assigned client websites only. Using a test account, observed the GWP Advisor™ logon process to determine whether access to client websites could only be obtained through a combination of the unique client website address, user name and password.	No exceptions noted.

5.13 Monitoring subservice organisations

Control Objective	Related Control	Frequency	Procedure	Results
G.13 Appointment of subservice organisations, including those providing IT services, are approved, subservice organisations are managed in accordance with the requirements of the client agreement and their activities are adequately monitored.	SS&C Technology Canada Corporation. Mississauga Data Centre: Report on the design of controls placed in operation and testing of operating effectiveness for the period October 1, 2021 to September 30, 2022. PricewaterhouseCoopers 2022. SS&C conforms to a formal due diligence process review for selecting third party providers. SS&C has a Risk Assessment plan to review third party service provider's security policies and procedures on a periodic basis. SS&C ensures that appropriate	Daily or many times daily	SS&C has a formal management information and reporting system that enables management to monitor key control and performance measurements for internal staff and external providers. A number of governance controls are in place to assess and validate the provision of services by subservice organisations, to ensure they meet agreed delivery metrics. Including the following:	No relevant deviations were noted.

Control Objective	Related Control	Frequency	Procedure	Results
	security clauses are incorporated into all third Party contracts which relate to the access, maintenance and upkeep of facilities. SS&C establishes and regularly updates procedures to limit and control third party access to information assets.		<p><u>Corporate Governance and Risk Management</u> SS&C has established a Board of Directors to oversee the business affairs of the company. The Board has a fiduciary duty to SS&C and its investors.</p> <p><u>Management's Philosophy and Operating Style</u> SS&C's operating and management style revolves around continuous communications between senior management and operating management. SS&C has an open door policy for employees, starting at the level of CEO.</p> <p>SS&C has established regular weekly meetings as a means for management to foster open communications throughout the company. The CEO conducts regular weekly meetings with his staff to review operating and strategic issues, as well as to review updates to financial and legal matters. In addition, a sales meeting occurs each week and is attended by both senior management and operating management. Department managers are also encouraged to establish regular departmental meetings in order to foster more open communications throughout the organisation</p> <p><u>Commitment to Competence</u> SS&C's objective is to hire employees with expertise in their area of responsibility and to provide them with the authority and responsibility to best perform their duties. SS&C encourages its managers to establish individual job responsibilities to best meet the objectives of its departments to cross-train employees to provide flexibility.</p>	

Control Objective	Related Control	Frequency	Procedure	Results
			<p>The candidates apply to SS&C by responding to job postings. The Human Resources department and hiring managers review the resumes in order to determine qualified candidates. Formal interviews and reference checks are completed where appropriate and background checks are performed for all candidates prior to a formal job offer being made. All job offers are reviewed and approved by senior management</p> <p><u>Controls Related to Personnel</u> SS&C has established policies and procedures for recruiting employees, the evaluation of job performance, remedial action for sub-standard performance or failure to adhere to policies, and employee conduct.</p> <p>All employees are hired based on the needs of the business and SS&C ensures that all parties understand the responsibilities of the position and the hiring process. The employee's manager determines any internal or external training requirements necessary for the newly hired employee to perform effectively in their job.</p> <p>SS&C utilizes a performance management system in order to evaluate employee performance and communicate this evaluation through regular performance reviews. The immediate supervisor or manager completes performance reviews annually for each of his or her direct reports. These are also reviewed and approved by the next level supervisor or manager. Performance issues are</p>	

Control Objective	Related Control	Frequency	Procedure	Results
			communicated directly to the employee by the supervisor or manager on a timely basis.	