Morgan Stanley

Report on the Internal Controls for Morgan Stanley Wealth Management Australia Pty Ltd Private Wealth Management Custody Services and Related Information Technology

ASAE 3402 audit for the period 1 August 2017 to 31 July 2018

December 2018

This report, including the description of tests of controls and results thereof is intended solely for the information and use of MSWM, user entities of MSWM's PWM custody services and related IT systems during some or all of the period, and the independent auditors of such user entities, who have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be and should not be used or relied upon by anyone other than these specified parties.

Table of contents

Section I:
Statement by the Service Organisation

Morgan Stanley

Section I: Statement by the Service Organisation

The accompanying description has been prepared for customers who have used the Private Wealth Management ("PWM") custody services and related information technology and their auditors who have a sufficient understanding to consider the description, along with other information including information about controls operated by customers themselves, when assessing the risks of material misstatements of customers' financial reports/statements. Morgan Stanley Wealth Management Australia Pty Ltd ("MSWM") confirms that:

(a) The accompanying description in Sections II and V fairly presents the PWM custody services and related information technology throughout the period 1 August 2017 to 31 July 2018. The criteria used in making this statement 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 customers.
- The related accounting records, supporting information and specific accounts that were used to initiate, record, process and report transactions; this includes the correction of incorrect information and how information was transferred to the reports prepared for customers.
- How the system dealt with significant events and conditions, other than transactions.
- The process used to prepare reports for customers.
- Relevant control objectives and controls designed to achieve those objectives.
- Controls that we assumed, in the design of the system, would be implemented by customers, and which, if necessary to achieve 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.
- 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 customers' transactions.

ii. Includes relevant details of changes to the service organisation's system during the period 1 August 2017 to 31 July 2018.

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 customers and their auditors and may not, therefore, include every aspect of the system that each individual customer may consider important in its own particular environment

(b) The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period 1 August 2017 to 31 July 2018. The criteria used in making this statement were that:

i. The risks that threatened achievement of the control objectives stated in the description were identified;

ii. The identified 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 that manual controls were applied by individuals who have the appropriate competence and authority, throughout the period 1 August 2017 to 31 July 2018.

Signed on behalf of Management of MSWM.

Astrid Ullmann

Chief Operating Officer
14 December 2018

Section II:
Description of the System accompanying the Statement by the Service Organisation

Section II: Description of the System accompanying the Statement by the Service Organisation

Introduction

This report is designed to provide information to be used for financial reporting purposes by the clients of Morgan Stanley Wealth Management Australia Pty Ltd ("MSWM"), their independent auditors and other persons authorised by MSWM. The information in this report is prepared in accordance with Standard on Assurance Engagements ASAE 3402 *Assurance Reports on Controls at a Service Organisation June 2014*, and with reference to the guidelines contained in Guidance Statement GS 007 *Audit Implications of the Use of Service Organisations for Investment Services October 2011* ("GS 007" or "the Guidance Statement"), issued by the Auditing and Assurance Standards Board (AUASB).

The report describes those controls that relate to the prescribed control objectives detailed in the Guidance Statement that pertain to the PWM custody services and related information technology.

1 Overview of Operations and Applicability of report

MSWM offers financial planning services, investment advice and stock broking services to Australian and overseas residents (generally high net worth) who wish to invest locally and internationally.
MSWM's international platform, known as 'Private Wealth Management' ("PWM") provides clients with access to a broad range of product offerings, including but not limited to international equities, fixed income products, foreign exchange products, listed options, over-the-counter derivatives, structured products, managed funds and other forms of offshore collective investment vehicles. Only clients that meet the Wholesale Client test under the *Corporations Act 2001* (Cth) are able to access the PWM platform.

1.1 General Overview of Company

The Company's immediate parent undertaking is Morgan Stanley Domestic Holdings Inc. The Company's ultimate parent undertaking and controlling entity is Morgan Stanley which, together with the Company and Morgan Stanley's other subsidiary undertakings, form the Morgan Stanley Group.
The Company is:

a) a registered Australian proprietary company (ACN 009 145 555);
b) the holder of an Australian Financial Service Licence (AFSL) (Licence Number 240813) issued by the Australian Securities & Investments Commission (ASIC);
c) a market participant of the financial market operated by the ASX Limited (ASX);
d) a clearing participant of ASX Clear Pty Limited; and
e) a settlement participant of ASX Settlement Pty Limited.

The Company is also a member of the Australian Financial Markets Association.

1.2 Structure of PWM

In respect of MSWM's PWM platform, MSWM acts as the introducing broker to a Morgan Stanley affiliate in the United Kingdom, Morgan Stanley & Co International plc (MSIP). That is, MSWM has a direct relationship with the clients of the PWM platform, and provides financial advice and certain administrative services to those clients, but MSIP is responsible for certain other functions, including the provision of custody services.

MSIP (FCA registration number 165935) is authorised by the Prudential Regulatory Authority ("PRA") and regulated by the PRA and the Financial Conduct Authority ("FCA") in the United Kingdom ("UK"). MSIP is subject to the rules of the FCA ("FCA Rules") with respect to holding of client assets, which supplement common law principles of trust. The FCA Rules exist to protect client assets held with an investment firm. FCA regulated financial services firms that hold client assets and client money are subject to the Client Asset Sourcebook section of the FCA Rules ("CASS"), which sets out the requirements relating to holding client assets and client money.

MSIP is exempt from the requirement in Australia to hold an AFSL under the *Corporations Act 2001* (Cth) in respect of the provision of certain financial services. When providing financial services to

Australian wholesale clients, MSIP does so through reliance on ASIC Class Order 03/1099: UK Regulated Financial Services Providers.

MSIP is registered as a foreign company in Australia (ARBN 613 032 705).

As noted above, MSIP is responsible for the provision of custody services in relation to assets held on the PWM platform. However MSIP does not accept orders or instructions directly from PWM clients – all instructions are placed through MSWM. MSWM is responsible for:

(a) accepting and transmitting orders and instructions regarding investments;
(b) approving, opening and monitoring PWM accounts including obtaining, verifying and retaining client account information and documents;
(c) determining whether persons placing instructions for the PWM accounts are authorised to do so;
(d) investigating and responding to any questions or client complaints related to the PWM accounts;
(e) maintaining the required books and records with respect to the functions it performs; and
(f) providing discretionary investment services in certain circumstances.

1.3 Applicability of Report

This report relates only to the business operated by MSWM and MSIP on the PWM platform. This report is intended to provide an understanding of the custody controls related to transactions in equities, fixed income, cash, mutual funds, alternative investments, foreign exchange products, listed options, over-the-counter derivatives, structured products, managed funds and other forms of offshore collective investment vehicles. The control functions are located in Sydney, London, Hong Kong, Singapore and the United States.
The report covers controls over the following areas with regard to accounts on the PWM platform:

- account set-up and account modification
- trading, trade support and settlement
- cash management
- deposits and payments
- security transfers
- errors handling
- investment income and corporate income
- reconciliation
- custody
- client reporting
- information system security
- information system operations
- application development and maintenance, and
- business continuity management.

For the above mentioned areas the operational and technology controls reside with MSWM and MSIP. Certain operational functions are performed by Morgan Stanley's Institutional Securities Group as part of a shared service centre.

With regards to the custody process, MSIP may outsource certain functions to sub-custodians as part of Morgan Stanley's global custody network. These outsourced functions are controlled by Morgan Stanley's Global Network Management department. The report does not extend to the controls at sub-custodians, which are detailed at Appendix 1.

Some MSWM clients have the custody service provided outside of Morgan Stanley by third party service providers. For these client relationships, the activities handled by third party service providers are outside the scope of this review as well.

2 Business Structure

MSWM is dedicated to serving clients through a relationship based on advice, integrity and mutual trust. When a new client comes to MSWM, the relationship begins with a discovery process; an in-depth dialogue to identify all the factors surrounding and defining the client's wealth. This includes the client's short and long-term goals and concerns, the structure of his or her holdings, and the client's exposure to, and tolerance for, risk.

The client's dedicated team, along with Morgan Stanley's wealth management specialists, then work with the client to construct, implement and monitor a service that will help the client achieve his or her objectives.

The MSWM business is divided in two key functions and responsibilities:

(a) Financial Advisers

Financial advisers are the client's primary point of contact. They work closely with clients to devise the appropriate investment approach. This may include developing and implementing a strategic asset allocation and risk management solution. Thereafter, financial advisers work with the client to meet their needs on a day-to-day basis. They ensure that any change in financial circumstances or risk profile is reflected in the construction of the portfolio. The financial advisers also provide access to Morgan Stanley's global research and trading franchise, and can provide additional investment solutions on an advisory basis.

(b) Administration, risk management, technology and support

MSWM provides financial advisers and their clients support through a number of business activities including the provision of investment research and products, holistic financial planning services and portfolio administration activities. On a day-to-day basis, risk management controls assist financial advisers to ensure that portfolios are being structured within agreed client risk tolerances. Oversight of the business is conducted at multiple layers by risk management, business management and autonomous compliance, legal and audit teams.

Through Morgan Stanley's technology platform clients can receive real-time access to their portfolios via a client web portal, called Matrix, as well as access to Morgan Stanley's published research.

3 Control environment and risk management

The control environment is an essential component of an organisation's governance structure and includes the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. The objectives of an internal control structure is to provide reasonable, but not absolute, assurance as to the integrity and reliability of the financial information, the protection of assets from unauthorised use or disposition, and that transactions are executed in accordance with management's authorisation and client instructions. The management of MSWM have established and maintained an internal control structure that monitors compliance with established policies and procedures.

MSWM's executive management are accountable to the Board of Directors of MSWM for monitoring the system of internal control within the business. MSWM's executive management have implemented an internal control system designed to facilitate effective and efficient operations. The control environment has been designed to enable management to respond appropriately to significant business, operational, financial, compliance and other risks. The system of internal control contributes to ensuring adequate control of internal and external reporting and compliance with applicable laws and regulations.

MSWM regards its internal control environment as fundamental to its business strategy. All business development initiatives are required to adhere to stringent control standards.

The controls and their related operation are described in more detail in Section V. In determining the controls and control objectives we took into account the following criteria:

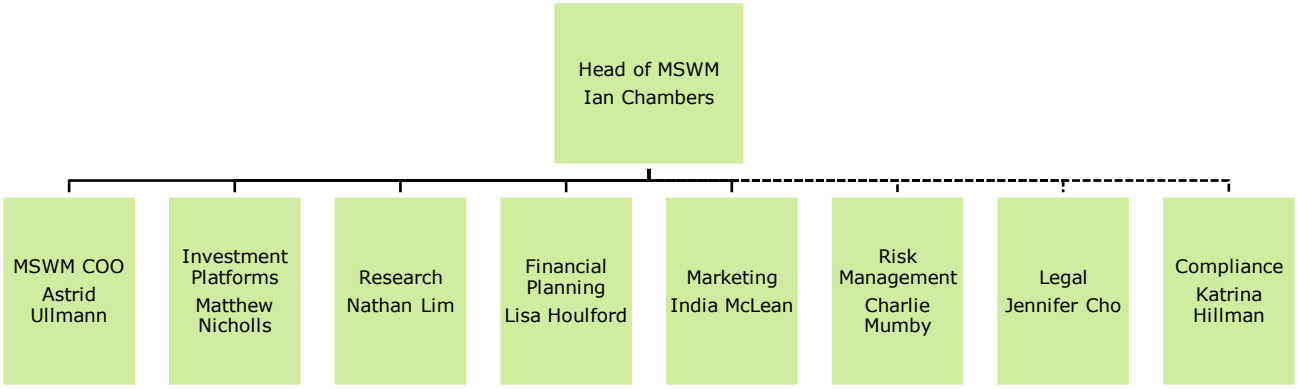
- The risks that threatened achievement of the control objectives stated in the description were identified;
- The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved; and
- The description of the controls and control environment does not omit relevant information.

3.1 Organisational Structure

MSWM's organisational structure provides a framework within which its business activities are planned, executed, controlled and monitored. A significant aspect of the set structure is defining key areas of authority and responsibility and establishing appropriate lines of reporting.

Organisational Chart

The organisational chart for the senior management of MSWM as at 31 July 2018 is shown below:



Functional Groups

The functional groups and their key responsibilities for areas in scope for this report are:

Group	Function
Branch Administration	Account set-up and modification Errors handling
Risk Management	Risk monitoring Business Continuity Management
Operations	New account set up Client reporting Trade support and settlement Deposit and payments Security transfers Reconciliation Investment income and corporate income Corporate actions Custody
Information Technology	Information system security Information system operations System development and maintenance
Sales & Marketing	Client interface Trading Cash management
Legal Entity Group	AML checks

3.2 Communication and Enforcement of Integrity and Ethical Values

For MSWM, maintaining an environment that demands integrity and ethical values is critical for the establishment and maintenance of an effectively controlled organisation. The effectiveness of internal controls cannot rise above the integrity and ethical values of the people who create, administer and monitor them. Therefore MSWM Board and Management promote integrity and ethical values.

MSWM as well as the whole of Morgan Stanley focuses on recruiting only high quality individuals for each position. MSWM provides specific rules, procedures and training for employees to fulfil the given tasks in the best interest of the organisation.

MSWM adheres to the Morgan Stanley codes and policies (such as Code of Conduct, Non-discrimination, and Anti-harassment policy) by requiring employees to read and acknowledge the codes and policies. Morgan Stanley conducts regular training and education sessions that are mandatory for employees. MSWM's management expect employees to maintain high moral and ethical standards.

Employees of MSWM have pre-clearance and reporting obligations with regards to employee securities accounts, personal securities transactions, outside activities, private placements, gifts and entertainment.

3.3 Assignment of Authority and Responsibility

The control environment is greatly influenced by the extent to which individuals recognise that they are held accountable. MSWM encourages individuals and teams to use initiative in addressing issues and solving problems. Management communicates, through various means (such as emails and meetings), its policies describing appropriate business practices to the staff.

3.4 Internal Audit Reviews

MSWM's risks and controls are reviewed by Morgan Stanley's Internal Audit department. Internal Audit evaluates the adequacy and effectiveness of controls over MSWM's governance, operations, and information systems. Audit reports, which carry an audit rating and outline the degree to which unacceptable risk exposures were identified, are presented to senior management. The audit reporting process actively considers and recommends ways in which control weakness may be corrected or risks may be mitigated. Management is required to respond to audit findings and to indicate target dates as to when appropriate corrective action will be completed.

3.5 Risk Management

Risk Management is responsible for the supervision and oversight of all aspects of MSWM risk, including market and non-market risks, and ensures that risks assumed are identified, understood and appropriately managed. Key risks facing the MSWM business are:

- Credit Risk: the most significant credit risk is that MSWM does not get paid back margin loans granted to clients (including risks associated with managing the collateral lodged by clients).
- Client Suitability Risk: the risk that MSWM faces financial loss as a result of selling products to clients for which they are not suitable (considered on both an upfront and ongoing basis).
- Product Suitability Risk the risk that MSWM faces financial loss as a result of Morgan Stanley doing insufficient due diligence on the products which it distributes to clients.
- Operational Risk: The risk that MSWM faces losses arising from failed or inadequate internal processes, systems or people, or from external events.

3.6 Information and Communication

Information and communication is integral to the continual competitiveness of an organisation. Morgan Stanley's management has policies and procedures in place to initiate, record, process, and report entity transactions and to effectively communicate and distribute relevant information timely. Both management and operations personnel are provided with an understanding of their individual roles and responsibilities pertaining to internal controls.

MSWM management encourage individuals and teams to use initiative in addressing issues and solving problems. Employees are made aware of changes to policies and procedures, significant business events and other major announcements by written communication (such as email). General Morgan Stanley announcements are communicated either through email or via Morgan Stanley's intranet. The employees are obligated to safeguard and prevent disclosure of sensitive, proprietary, confidential, privileged, or secret information. MSWM has various policies in place governing this.

3.7 Monitoring

An important management responsibility is to establish and maintain internal controls and to monitor business developments on an ongoing basis. MSWM management reviews such areas through various metric figures, reviews and committees.

4 Operations and infrastructure support model controls

MSWM relies in part on Morgan Stanley's support infrastructure to conduct its business through the outsourcing of some services and systems.
Services that are provided to MSWM by MSIP (and other entities of the Morgan Stanley Group) include:

- information technology
- operations
- legal and compliance
- risk management
- tax
- human resources

- financial and regulatory controls, and
- treasury

As part of the delegated operations services, certain activities to support the delivery of custody services such as the handling of corporate actions and dividends/income, and the segregation of assets are delegated to Morgan Stanley's ISG Operations as outlined below:

- Morgan Stanley ISG Operations handles for MSWM PWM customers the receipt and distribution of dividends and other distributions, the processing of exchange offers, right offerings, warrants, tender offers, exercises, calls, redemptions and sales and transfers of shares subject to any applicable restriction, other corporate actions and such other functions
- Morgan Stanley ISG Operations ensures the segregation of client assets and firm assets in line with FCA regulations. The Operations team protects positions by keeping client assets in a segregated safekeeping account.

5 IT systems

5.1 Network and Infrastructure

Morgan Stanley PWM utilizes both mainframe and distributed technology. The key system platforms are standardized on z/OS, Linux and Windows operating systems. Morgan Stanley owns and operates the Data Centres located in Somerset, New Jersey, Piscataway, New Jersey, and Ashburn, Virginia.

5.2 Information Technology Organisation

Morgan Stanley IT is divided into the business units with a New York based IT Senior Manager heading up PWM IT from a global perspective while global functional heads report to the New York based IT Senior Manager. Some of the functional heads also have a regional responsibility, in which case they also report to local business heads in their regional offices. Staff working on global projects will have a link, organized by function, to the functional area that is leading and managing that project.

Morgan Stanley's Enterprise Infrastructure Group ("EI") is responsible for each business line's server management and deployment needs, providing adherence to Morgan Stanley IT standards. PWM is a business line under the responsibility of the Engineering/service account manager for PWM. While the responsibility is centralized, the specialized support groups are resident in each location. Specialized groups include Network, UNIX, Windows and database support. The IT functions generally operate based on firm wide standards. There are policies and procedures for many functions set by Quality Assurance and Production Management (QAPM).

Production Management is responsible for supporting PWM applications and ensuring the stability of the IT environment. Responsibilities include application support, software turnovers/deployments and monitoring of overnight batch processes. ASG personnel are located across several regions which ensures that there is coverage throughout the day and night.

In-bound instructions to Ausmaq are received electronically via Webstreme - a secure order management system developed by Ausmaq. An ASAE 3402 Assurance Report on Controls at a Service Organisation has been received along with Ausmaq's "Report on the Internal Controls for Custody, Investment Administration and Related Information Technology Services".

Section III:
Independent Service Auditor's Assurance Report on the Description of Controls, their Design and Operating Effectiveness

Deloitte Touche Tohmatsu
ABN 74 490 121 060

550 Bourke Street
Melbourne VIC 3000
GPO Box 78
Melbourne VIC 3001 Australia

Tel: +61 3 9671 7000
Fax: +61 3 9671 7001
www.deloitte.com.au

Deloitte.

Section III: Independent Service Auditor's Assurance Report on the Description of Controls, their Design and Operating Effectiveness

To the Directors of Morgan Stanley Wealth Management Pty Ltd ("MSWM")

Scope

We have been engaged to report on MSWM's description of its internal controls over Private Wealth Management's ("PWM") custody services and related information technology throughout the period from 1 August 2017 to 31 July 2018 (the description), and on the design and operation of controls related to the control objectives stated in the description.

MSWM's Responsibilities

MSWM is responsible for: preparing the description and accompanying statement in Section I, including the completeness, accuracy and method of presentation of the description and statement; providing the services covered by the description; stating the control objectives; and designing, implementing and effectively operating controls, as disclosed in the controls matrix in Section V, to achieve the stated control objectives.

Our Independence and Quality Control

We have complied with relevant ethical requirements related to assurance engagements, which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

The firm applies Auditing Standard ASQC 1 *Quality Control for Firms that Perform Audits and Reviews of Financial Reports and Other Financial Information, Other Assurance Engagements and Related Services Engagements* and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on MSWM'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*, issued by the Auditing and Assurance Standards Board. That standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented and the controls 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 Section I.

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

MSWM PWM's description is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of the system that each individual customer may consider important in its own particular environment. Also, because of their nature, controls at a service organisation may not prevent or detect 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 V. In our opinion, in all material respects:

(a) The description fairly presents the MSWM PWM custody services and related information technology as designed and implemented throughout the period from 1 August 2017 to 31 July 2018;

(b) The controls related to the control objectives stated in the description were suitably designed throughout the period from 1 August 2017 to 31 July 2018; 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 August 2017 to 31 July 2018.

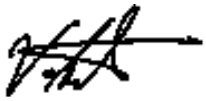
Description of Tests of Controls

The specific controls tested and the nature, timing and results of those tests are listed in Section V.

Intended Users and Purpose

This report and the description of tests of controls in Section V are intended only for customers who have used MSWM's PWM custody services and related information technology, and their auditors, who have a sufficient understanding to consider it, along with other information including information about controls operated by customers themselves, when assessing the risks of material misstatements of customers' financial reports/statements.

DELOITTE TOUCHE TOHMATSU



Vincent Sita
Partner
Chartered Accountants
14 December 2018

Section IV:
Overview of the Work Performed

Deloitte.

Section IV: Overview of the Work Performed

Introduction

This report on the description of the system is intended to provide user entities (customers) and their auditors with information for their evaluation of the effect of a service organisation on a customer's internal control relating to MSWM's controls over the PWM custody services and related information technology throughout the period 1 August 2017 to 31 July 2018.

Deloitte's examination was conducted in accordance with the Standard on Assurance Engagements 3402, *Assurance Reports on Controls at a Service Organisation*, issued by the Auditing and Assurance Standards Board. Our testing of MSWM PWM's controls was restricted to the control objectives and related control activities listed in Section V and was not extended to controls described in Section II but not included in Section V, or to controls that may be in effect at user organisations.

Deloitte's work was carried out at the premises of Morgan Stanley in Sydney and in other primary geographies including New York, Hong Kong and London. The scope of our work was based on criteria (control objectives) agreed with management of MSWM prior to the commencement of our work.

The report does not extend to the controls at sub-custodians, which are detailed at Appendix 1.

Control environment elements

The control environment sets the tone of an organisation, influencing the control consciousness of its people. It is the foundation for other components of internal control, providing discipline and structure. In addition to the tests of design, implementation, and operating effectiveness of controls identified by MSWM, Deloitte's procedures included tests of the following relevant elements of MSWM's control environment:

a. account set-up and account modification
b. trading, trade support and settlement
c. cash management
d. deposits and payments
e. security transfers
f. errors handling
g. investment income and corporate income
h. reconciliation
i. custody
j. client reporting
k. information system security
l. information system operations
m. application development and maintenance, and
n. business continuity management.

Such tests included inquiry of the appropriate management, supervisory, and staff personnel; observation of MSWM's activities and operations, inspection of MSWM's documents and records, and re-performance of the application of MSWM's controls. The results of these tests were considered in planning the nature, timing, and extent of testing of the control activities described in Section V.

Tests of operating effectiveness

Our tests of the controls were designed to cover a representative number of transactions throughout the period from 1 August 2017 to 31 July 2018. In determining the nature, timing and extent of tests we considered the following:

(a) Nature and frequency of the controls being tested
(b) Types of available evidential matter
(c) Nature of the control objectives to be achieved
(d) Assessed level of control risk
(e) Expected effectiveness of the test, and
(f) Results of our tests of the control environment.

Testing the accuracy and completeness of information provided by MSWM is also a component of the testing procedures performed. Information we utilised as evidence may have included, but was not limited to:

- Standard "out of the box" reports as configured within the system
- Parameter-driven reports generated by MSWM's systems
- Custom-developed reports that are not standard to the application such as scripts, report writers, and queries
- Spreadsheets that include relevant information utilized for the performance or testing of a control
- MSWM prepared analyses, schedules, or other evidence manually prepared and utilized by MSWM.

While these procedures may not be specifically called out in the test procedures listed in Section V, they may be completed as a component of testing to support the evaluation of whether or not the information is sufficiently precise and detailed for purposes of fully testing the controls identified by MSWM.

Description of testing procedures performed

Deloitte Touche Tohmatsu ("Deloitte") performed a variety of tests relating to the controls listed in Section V throughout the period from 1 August 2017 to 31 July 2018. Our tests of controls were performed on controls as they existed during this period and were applied to those controls relating to control objectives specified by MSWM.

Tests performed for the purpose of this report may have included, but were not limited to those described below:

Test	Description
Corroborative Inquiry	Conducted detailed interviews with relevant personnel to obtain evidence that the control was in operation during the report period and is accompanied by other procedures noted below that are necessary to corroborate the information derived from the inquiry.
Observation	Observed the performance of the control multiple times throughout the report period to evidence application of the specific control activity.
Inspection of documentation	If the performance of the control is documented, inspected documents and reports indicating performance of the control.
Reperformance of monitoring activities or manual controls	Obtained documents used in the monitoring activity or manual control activity and independently reperformed the procedures. Compared any exception items identified with those identified by the responsible control owner.
Reperformance of programmed processing	Input test data, manually calculated expected results, and compared actual results of processing to expectations.

Sampling Methodology

In terms of frequency of the performance of the control by MSWM, we consider the following guidance when planning the extent of tests of control for specific types of control.

(g) The purpose of the procedure and the characteristics of the population from which the sample will be drawn when designing the sample;
(h) Determine a sample size sufficient to reduce sampling risk to an appropriately low level;
(i) Select items for the sample in such a way that each sampling unit in the population has a chance of selection;

(j) If a designed procedure is not applicable to a selected item, perform the procedure on a replacement item; and
(k) If unable to apply the designed procedures, or suitable alternative procedures, to a selected item, treat that item as a deviation.

Where a manual control is performed periodically or is recurring, the following guidelines are at a minimum followed in performing the test of controls:

Frequency of control activity	Minimum sample size for a period of 12 months
Annual	1
Quarterly	2
Monthly	2
Weekly	5
Daily	15
Recurring manual control (multiple times per day)	25
Automated Controls	Test one instance of each automated control.
Indirect Controls (e.g., indirect entity-level controls, general IT controls)	For those indirect entity-level controls that do not themselves directly address risks of material misstatement, the above is the suggested minimum sample size for the test of operating effectiveness. In the event that the indirect control is directly responsive to the control objective, the above is the minimum sample size for the test of operating effectiveness.
The table assumes zero deviations.	

The nature and cause of deviations (if any) are identified and evaluated whether the rate of deviation is acceptable, additional testing of that or another control is necessary or that the testing provides an appropriate basis for concluding the control is not effective for the period of reliance.

General IT controls may be manual, manual with an automated component or automated. Where a general IT control is manual or manual with an automated component, the guidelines above related to the extent of testing of manual controls are considered to determine the extent of testing of general IT controls. Where a general IT control is automated, we use our professional judgement, combined with the guidance above keeping in consideration that due to the inherent consistency of IT processing, it may not be necessary to increase the extent of testing of an automated control and that an automated control can be expected to function consistently unless the program is changed.

Reporting on results of testing

In most instances, controls are performed in the same manner and with the same degree of intensity for all clients. For this reason, samples were chosen from the whole population of MSWM transactions. Deloitte does not have the ability to determine whether a deviation will be relevant to a particular user, consequently all deviations are reported.

Results of testing

The concept of effectiveness of the operation of controls recognises that some exceptions in the way controls are applied by MSWM may occur. Exceptions from prescribed controls may be caused by such factors as changes in key personnel, significant seasonal fluctuations, volume of transactions and human error.

We use judgement in considering the overall operating effectiveness of the control by considering the number of exceptions detected, the potential significance of the financial statement effect, as well as other qualitative aspects of the exceptions such as the cause of the exception.

When we identify an exception for a periodic or automated control, we consider whether other controls may provide the evidence we require.

When we identify an exception for a recurring manual control, we consider whether:

- To increase the extent of testing to be performed; and/or
- Other controls that may provide the evidence we require.

If we find a single deviation in our initial sample for a recurring manual control operating multiple times per day, when we did not expect to find control deviations, we consider whether the deviation is representative of systematic or intentional deviations.

If control deviations are found in tests of controls which operate daily or less frequently, the sample size cannot be extended and we assess such controls as ineffective.

Executive Summary

Control Objective	Number of controls effectively designed and implemented and operating effectively	Total number of controls per objective	Result
A.1 New accounts are set up completely and accurately in accordance with client agreements and any applicable regulations.	2	2	Control objective met
A.2 Complete and authorised client agreements are established prior to initiating custody activity.	1	1	Control objective met
A.3 Investment and related cash and foreign exchange transactions are authorised and recorded completely, accurately and on a timely basis in accordance with client instructions.	4	4	Control objective met
A.4 Investment and related cash and foreign exchange transactions are settled completely, accurately and on a timely basis and failures are resolved in a timely manner.	2	2	Control objective met
A.5 Corporate actions are identified, actioned, processed and recorded on a timely basis.	3	3	Control objective met
A.6 Cash receipts and payments are authorised, processed and recorded completely, accurately and on a timely basis	2	2	Control objective met
A.7 Securities lending programs are authorised and loan initiation, maintenance and termination are recorded on an accurate and timely basis.	N/A	N/A	Not applicable.
A.8 Loans are collateralised in accordance with the lender's agreement and the collateral together with its related income is recorded completely, accurately and on a timely basis.	N/A	N/A	Not applicable.
A.9 Collateral is completely and accurately invested in accordance with the lender's agreement.	N/A	N/A	Not applicable.
A.10 Accounts are administered in accordance with client agreements and any applicable regulations.	3	3	Control objective met
A.11 Changes to non-monetary static data (for example, address changes and changes in allocation instructions) are authorised and correctly recorded on a timely basis.	2	2	Control objective met
A.12 Investment income and related tax reclaims are collected and recorded accurately and on a timely basis.	3	3	Control objective met

A.13 Asset positions for securities held by third parties such as sub custodians and depositories are accurately recorded and regularly reconciled.	2	2	Control objective met
A.14 Assets held (including investments held with depositories, cash and physically held assets) are safeguarded from loss, misappropriation and unauthorised use.	4	4	Control objective met
A.15 Assets held are appropriately registered and client money is segregated.	1	1	Control objective met
A.16 Transaction errors are rectified promptly.	3	3	Control objective met
A.17 Appointments of subservice organisations, including sub-custodians, are approved, subservice organisations are managed in accordance with the requirements of the client agreement and their activities are adequately monitored.	3	3	Control objective met
A.18 Client reporting in respect of client asset holdings is complete and accurate and provided within required timescales.	3	3	Control objective met
A.19 Asset positions and details of securities lent (including collateral) are reported to interested parties accurately and within the required time scale.	N/A	N/A	Not applicable.
G.1 Physical access to computer networks, equipment, storage media and program documentation is restricted to authorised individuals.	1	1	Control objective met
G.2 Logical access to computer systems, programs, master data, client data, transaction data and parameters, including access by administrators to applications, databases, systems and networks, is restricted to authorised individuals via information security tools and techniques.	4	4	Control objective met
G.3 Segregation of incompatible duties is defined, implemented and enforced by logical security controls in accordance with job roles.	5	5	Control objective met
G.4 IT processing is authorised and scheduled appropriately and deviations are identified and resolved in a timely manner.	2	2	Control objective met
G.5 Appropriate measures, including firewalls and anti-virus software, are implemented to counter the threat from malicious electronic attack.	1	1	Control objective met
G.6 The physical IT equipment is maintained in a controlled environment.	1	1	Control objective met
G.7 Development and implementation of new systems, applications and software, and changes to existing systems, applications and Software, are authorised, tested, approved, implemented and documented.	5	5	Control objective met
G.8 Data migration or modification is authorised, tested and, once performed, reconciled back to the source data.	1	1	Control objective met

G.9 Data and systems are backed up regularly offsite and regularly tested for recoverability on a periodic basis.	1	1	Control objective met
G.10 IT hardware and software issues are monitored and resolved in a timely manner.	1	1	Control objective met
G.11 Business and information systems recovery plans are documented, approved, tested and maintained.	1	1	Control objective met
G.12 Information Technology services provided to clients are approved, managed and performance thresholds met in accordance with the requirements of the client agreement.	N/A	N/A	Not applicable.
G.13 Appointment of sub-service 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.	1	1	Control objective met

Section V:
Control Objectives, Control Activities, Testing of Design and Implementation and Operating Effectiveness

Section V:
Control Objectives, Control Activities, Testing of Design and Implementation and Operating Effectiveness

Introduction

This section presents the following information provided by MSWM:

- The control objectives specified by the management of MSWM.
- The process described by the management of MSWM.
- The controls established and specified by MSWM to achieve the specified control objectives.

Also included in this section is the following information provided by Deloitte Touche Tohmatsu:

- A description of the tests performed by Deloitte Touche Tohmatsu to determine whether MSWM's controls were operating with sufficient effectiveness to achieve specified control objectives. Deloitte Touche Tohmatsu determined the nature, timing, and extent of the testing performed.
- The results of Deloitte Touche Tohmatsu's tests of controls.

It is each user's responsibility to evaluate the information included in this report in relation to internal control in place at individual user entities to obtain an understanding and to assess control risk at the user entities. The controls at user entities and MSWM's controls should be evaluated together. If effective user entity controls are not in place, MSWM's controls may not compensate for such weaknesses.

Controls that are performed by MSWM's users remain their responsibility and were not considered as part of this engagement.

Controls Matrix

The following represents the MSWM Directors' description of control objectives and controls over custody services and related information technology, and the auditor's description of the nature, timing and extent of auditor testing of controls and deviations identified. All controls were in operation for the period from 1 August 2017 to 31 July 2018.

Custody

Accepting Clients

Control Activity	Service Auditor's Description of the Nature, Timing and Extent of Tests Applied to Controls	Results of Tests
A.1 – New accounts are set up completely and accurately in accordance with client agreements and any applicable regulations.		
A. An account opening form is signed off by the Branch Administration Management (BAM) Team after reviewing information provided and ensuring that Legal and AML (if required) reviews were performed.	**Inspection** Inspected a sample of account opening forms and evidenced sign off from BAM and Legal entities AML (Compliance) reviewed when required.	No relevant deviations noted.
B. The set-up of client accounts in the system is performed by the Operations team and reviewed by a supervisor, who signs off on the account opening checklist.	**Inspection** Inspected a sample of account opening checklists and verified completion and sign off by a supervisor.	No relevant deviations noted.
A.2 – Complete and authorised client agreements are established prior to initiating custody activity.		
A. The General Terms form is signed off by the client prior to an account system set up.	**Inspection** Inspected a sample of General Terms forms and verified sign off by the client prior to an account system set up.	No relevant deviations noted.

Authorising and processing transactions

Control Activity	Service Auditor's Description of the Nature, Timing and Extent of Tests Applied to Controls	Results of Tests
A.3 – Investment and related cash and foreign exchange transactions are authorised and recorded completely, accurately and on a timely basis in accordance with client instructions.		
A. Trade Processing Once trades have been executed by the Financial Adviser, a contract note is automatically generated by the system and provided to the client.	**Observation** Observed an automated generation of a contract note after trade details had been entered into the system along with the contract note being provided to the client.	No relevant deviations noted.
B. Payment Processing All payment instructions are signature verified by BAM - these include Standing Letters of Authority.	**Inspection** Inspected a sample of payment instructions and evidenced checks on letters of authority and approval provided to Operations by BAM.	No relevant deviations noted.
C. There is a segregation of duties when BAM approves and Operations processes payments requests via the SAFE system.	**Inspection** Inspected a sample of payment instructions and evidenced segregation between who processed the payments and who approved those payments.	No relevant deviations noted.
D. A "four eye" check for amounts that are < USD1M and "six eye" check (inputter and two authorizers) for amounts > USD1M. Both inputter and authorizer(s) will validate the completeness and accuracy of the instructions.	**Inspection** Inspected a sample of input of transactions and evidenced review to ensure accuracy and completeness according to client instructions as well as appropriate four eyes/six eyes checks.	No relevant deviations noted.

Control Activity	Service Auditor's Description of the Nature, Timing and Extent of Tests Applied to Controls	Results of Tests
A.4 – Investment and related cash and foreign exchange transactions are settled completely, accurately and on a timely basis and failures are resolved in a timely manner.		
A. SAFE automatically identifies daily settlement exceptions for the population of trades.	**Observation** Observed that SAFE system automatically identifies settlement exceptions.	No relevant deviations noted.
B. Agent cash and stock activities are reconciled by the Reconciliations Utility team. Outstanding breaks will be assigned by the Settlement team to appropriate teams for investigation and resolution.	**Inspection** Inspected a sample of reconciliations and evidenced follow up on trade breaks by the settlements team.	No relevant deviations noted.
A.5 – Corporate actions are identified, actioned, processed and recorded on a timely basis.		
A. Exception Report A workflow tool records all incoming SWIFTs (Corporate Action notices) from the local custodians. There is an exception report auto-generated from the workflow system twice per week. This report highlights all the events that have not been set up. The team manager reviews this report and ensures exceptions are cleared.	**Inspection** Inspected a sample of exceptions report and evidenced that breaks were individually reviewed.	No relevant deviations noted.
B. Reconciliation on Corporate actions Settlement team validates announcements against the information received from local custodian or exchanges as additional control before sending the notification to the entitled shareholders.	**Inspection** Inspected a sample of announcements validated against local custodian and Firm's internal systems before sending the notification to the shareholders.	No relevant deviations noted.

Control Activity	Service Auditor's Description of the Nature, Timing and Extent of Tests Applied to Controls	Results of Tests
C. Upon payment, Operations reconcile the cash/stock outturn versus an internal calculation and reflect the corporate action (CA) economics in the books and records.	**Inspection** Inspected a sample of reconciliations between the cash/stock outturn and internal calculation and evidenced that key positions and payments were properly reconciled and approved, with the CA economics reflected in the books and records.	No relevant deviations noted.
A.6 – Cash receipts and payments are authorised, processed and recorded completely, accurately and on a timely basis.		
Refer to A.3 for controls related to cash transactions.		
A. Payment and receipt requests are processed and validated through systemic maker and checker process. Any exception will require additional validation before instructions are released to the agent.	**Inspection** Inspected a sample of cash receipts/payments requests and related status emails from maker to checker evidencing execution status and any follow-ups as necessary.	No relevant deviations noted.
B. Operations will tally all requests received against system entries to ensure completeness. Approval and exception queues are checked to ensure all requests for the day are fully validated in the system.	**Inspection** Inspected a sample of cash receipts/payments requests and evidenced that all requests in the system had an associated downstream status. A sign off was also provided in a report acknowledging completion of task.	No relevant deviations noted.
A.7 – Securities lending programs are authorised and loan initiation, maintenance and termination are recorded on an accurate and timely basis.		
Not applicable, securities base lending is currently not offered to clients.		

Maintaining financial and other records

Control Activity	Service Auditor's Description of the Nature, Timing and Extent of Tests Applied to Controls	Results of Tests
A.8 – Loans are collateralised in accordance with the lender's agreement and the collateral together with its related income is recorded completely, accurately and on a timely basis.		
Not applicable for the period.		
A.9 – Collateral is completely and accurately invested in accordance with the lender's agreement.		
Not applicable for the period.		
A.10 – Accounts are administered in accordance with client agreements and any applicable regulations.		
Ongoing reviews are carried out to ensure that a client's investments are in line with pre-determined limits. These limits have been set as part of the client on-boarding process and are based on their risk tolerance and suitability for certain investment types. A. The firm's risk systems monitor all client holdings as well as pre- and post-trade checks. Any breaches of these checks are automatically highlighted to the financial adviser. Breaches are escalated by the Risk team if not resolved in a timely manner.	**Observation** Observed that the system has been set up to consistently monitor compliance with client rules based on the agreed risk tolerance and suitability of investments. **Inspection** Inspected a sample of an automated e-mail from the system to the Financial adviser, containing breach specifications, and a follow up e-mail to the Risk team requiring further action.	No relevant deviations noted.
B. The Compliance team perform quarterly reviews of daily surveillance completed by the PWM BAM in relation to trading by MSWM clients on the PWM platform, to ensure adherence to appropriate regulatory requirements and SLAs.	**Inspection** Inspected a sample of quarterly dashboard reviews performed by the Compliance team and evidenced assessment of financial advisor activities and outcomes.	No relevant deviations noted.

Control Activity	Service Auditor's Description of the Nature, Timing and Extent of Tests Applied to Controls	Results of Tests
C. The Compliance Monitoring Inventory system (CMI) is where monitoring alerts are maintained globally. Alerts related to trading by MSWM clients on the PWM platform are published to the Actimize system where the oversight function is performed by Compliance.	**Observation** Observed that alerts are kept on the CMI system and transferred to Actimize for oversight function performed by BAM and Compliance.	No relevant deviations noted.
A.11 – Changes to non-monetary static data (for example, address changes and changes in allocation instructions) are authorised and correctly recorded on a timely basis.		
A. Instructions received from clients are verified by the Fund Adviser or CSA, who completes a change request form and submits the form to BAM for approval. For changes that don't require client consent, instructions are communicated through e-mail by BAM. Amendments are done in the system by Operations, after BAM approval.	**Inspection** Inspected a sample of change requests and in each case evidenced completion of a change request form approved by BAM or e-mail from BAM to Operations, requesting amendments.	No relevant deviations noted.
B. A checklist of changes processed by the maker is reviewed and signed off by a supervisor, who compares changes to the client change request documentation.	**Inspection** Inspected a sample of checklists of changes and evidenced review and sign off from a supervisor, to ensure records are correctly recorded on a timely basis.	No relevant deviations noted.
A.12 – Investment income and related tax reclaims are collected and recorded accurately and on a timely basis.		
Investment Income - Refer to A.5 for Investment Income Recording. Tax Reclaims – MSWM does not provide a reclaim service for clients.		

Control Activity	Service Auditor's Description of the Nature, Timing and Extent of Tests Applied to Controls	Results of Tests
A.13 – Asset positions for securities held by third parties such as sub custodians and depositories are accurately recorded and regularly reconciled.		
A. A reconciliation between bank statements and internal books and records (TAPS) is performed using the reconciliation tool Intellimatch. Logic is incorporated to allow for automated matching and assignment of remaining breaks. Following the automated process, any pending break is reviewed by the global reconciliation team to identify further potential matching or assign them to the appropriate Business units for resolution.	**Inspection** Inspected a sample of reconciliations on asset/ cash positions held by third parties and evidenced that discrepancies are followed up by the global reconciliation team, investigated and assigned for resolution.	No relevant deviations noted.
B. In the event of a Stock positon break and Cash balances break, Intellimatch, a settlement exception monitoring system, will automatically flag up as a mismatch. MS settlement teams will be notified by Intellimatch and will reach out to the respective operations teams to further investigate on the booking.	**Observation** Observed that Intellimatch automatically generates an e-mail notification when breaks are identified, during the system reconciliation. Evidenced follow up from the Settlements team to business units for investigation and resolution of breaks.	No relevant deviations noted.

Safeguarding assets

Control Activity	Service Auditor's Description of the Nature, Timing and Extent of Tests Applied to Controls	Results of Tests
A.14 – Assets held (including investments held with depositories, cash and physically held assets) are safeguarded from loss, misappropriation and unauthorised use.		
A. Custodian Agreements with Asset Segregation letters are in place for all Client Custody accounts as well as Trust Acknowledgement Letters for all Client Money locations.	**Inspection** Inspected Custodian Agreements and Asset Segregation letters to evidence segregation of client money and responsibilities. Inspected Trust Acknowledgement Letters to evidence the rules set out in the CASS were followed.	No relevant deviations noted.
B. There is an annual due diligence programme in place for all agent banks, custodian and brokers, holding client money, in scope of CASS - custodian rules faced by MSIP in UK.	**Inspection** Inspected a sample of custodians, banks and brokers' annual due diligence and risk assessment performed under scope of CASS.	No relevant deviations noted.
C. Matters related to assets held by third parties are discussed during the monthly Assets Governance Committee meeting.	**Inspection** Inspected a sample of monthly minutes and evidenced that Client money and Assets are an agenda item of the meeting, however, no material issues or concerns were raised.	No relevant deviations noted.
D. Internal and External Reconciliations: Daily Reconciliations are in place to confirm Internal books and Records match Agents records. Breaks and discrepancies are fully investigated until resolution.	**Inspection** For external reconciliations, refer to A13A. Inspected a sample of internal reconciliations between internal and external Agents records and evidenced that discrepancies were investigated.	No relevant deviations noted.

A.15 – Assets held are appropriately registered and client money is segregated.
Refer to testing under A14.A

Monitoring compliance

Control Activity	Service Auditor's Description of the Nature, Timing and Extent of Tests Applied to Controls	Results of Tests
A.16 – Transaction errors are rectified promptly.		
A. The financial adviser must inform BAM as soon as they become aware of an error. Where there is market exposure, BAM will immediately instruct for correcting trades to be placed. The financial adviser has to complete and sign off on an error form, detailing the reason for the error. The error form is checked and signed off by BAM who instruct Operations team to rebook error trades to the relevant error account as soon as possible.	**Inspection** Inspected a sample of error forms and evidenced sign off/approval by BAM and instructions sent to operations for rectification.	No relevant deviations noted.
B. The financial adviser must inform BAM as soon as they become aware of the necessity of cancel/correction the trade. The financial adviser has to complete and sign off on a cancel and correction request form, detailing the reason for the cancels and corrections. The cancel/correction form is checked and signed off by BAM who instruct Operations team to rectify trades as soon as possible.	**Inspection** Inspected a sample of cancel and correction forms and evidenced sign off/approval by BAM and instructions sent to operations for rectification. Evidenced follow up from the BAM team for investigation and resolution of outstanding rectification.	No relevant deviations noted.

Control Activity	Service Auditor's Description of the Nature, Timing and Extent of Tests Applied to Controls	Results of Tests
C. Operations perform real-time daily trade reconciliation of the wash accounts, which both the client and execution trades are booked against, to ensure the accuracy of all bookings. Breaks are investigated and steps taken to resolve. Breaks reports are reviewed and signed off by the Supervisor daily.	**Inspection** Inspected a sample of real time reconciliations and break reports (between Equity and Fixed Income products) signed off by the supervisor and followed up for resolution.	No relevant deviations noted.

Monitoring Subservice Organisations

Control Activity	Service Auditor's Description of the Nature, Timing and Extent of Tests Applied to Controls	Results of Tests
A.17 – Appointments of subservice organisations, including sub-custodians, are approved, subservice organisations are managed in accordance with the requirements of the client agreement and their activities are adequately monitored.		
A. MS Global Network Management team assess custodians and agent banks suitability on an ad-hoc basis, based on a list of considerations.	Confirmed with Management that there was only one new subservice organisation during the period (Ausmaq) providing registry services. **Inspection** Inspected a sample of due diligence questionnaires sent to custodians/agent banks in the year, and verified that MSWM had reviewed the responses in its assessment of suitability. Inspected Ausmaq's GS 007 and Business Continuity Plan.	No relevant deviations noted.

Control Activity	Service Auditor's Description of the Nature, Timing and Extent of Tests Applied to Controls	Results of Tests
	For the Annual Due Diligence of providers, refer to A14.B.	
B. MS Global network Management team produce a risk rating annual market report for the custodians and agent banks in question.	**Inspection** Inspected a sample of annual market reports and evidenced that risk rating was produced for the custodian/bank in question. A checklist was signed off by the reviewer to ensure completeness.	No relevant deviations noted.
C. Incidents with providers are logged into the Global system and monitored until resolution.	**Inspection** Inspected a sample of incidents and obtained evidence of recording and monitoring in the Global Incident Network.	No relevant deviations noted.

Reporting

Control Activity	Service Auditor's Description of the Nature, Timing and Extent of Tests Applied to Controls	Results of Tests
A.18 – Client reporting in respect of client asset holdings is complete and accurate and provided within required timescales.		
A. Daily position and balance reconciliation on client asset holdings between client reporting database and upstream feed is carried out throughout the day. Any exceptions are highlighted in the exception monitoring tool, so errors can be cleared without blocking clients' accounts.	**Observation** Observed, for an automated reconciliation, that breaks identified during the automated daily position and balance reconciliation are highlighted in the Exception Monitoring tool, for investigation and resolution.	No relevant deviations noted.

Control Activity	Service Auditor's Description of the Nature, Timing and Extent of Tests Applied to Controls	Results of Tests
B. Monthly Asset under Management (AUM) figures are verified and sample checked against the month end official statement generated.	**Inspection** Inspected monthly asset under management reports and evidenced checks performed against the official statement, with discrepancies investigated.	No relevant deviations noted.
C. Monthly statement delivery reconciliation is performed to ensure that at least 99% of client statements are sent by the end of the following month. Statement exceptions are identified and reviewed until all client statements are sent.	**Inspection** Inspected monthly statement delivery reconciliations and evidenced that over 99% of physical and electronic statements were sent to clients during the following month.	No relevant deviations noted.
A.19 – Asset positions and details of securities lent (including collateral) are reported to interested parties accurately and within the required time scale.		
Not applicable, securities base lending are currently not offered to clients.		

Information Technology

Control Activity	Service Auditor's Description of the Nature, Timing and Extent of Tests Applied to Controls	Results of Tests
G1: Physical Access to computer networks, equipment, storage media and program documentation is restricted to authorised individuals.		
A. Access to the building and immediate surroundings of computer equipment is restricted to individuals who require such access to perform their job responsibilities and is monitored. Information technology management approval is required before access is granted.	**Observation** Observed the data centre facilities and confirmed access is restricted by the use of key card access systems and/or biometric systems based on users' roles and responsibilities. **Inspection** Inspected a sample of tickets from a listing of new data centre users during the audit period and evidenced that access had been approved. **Inspection** Inspected a sample of monthly review reports for inactive users for each data centre and evidenced that a review was performed and access was revoked.	No relevant deviations noted.
	Webstreme (Ausmaq Third party software) **Inspection** Inspected the Ausmaq ASAE 3402 report regarding the effectiveness of internal controls related to physical access policies, physical access, storage of media and datacentre security devices.	No relevant deviations noted.

Control Activity	Service Auditor's Description of the Nature, Timing and Extent of Tests Applied to Controls	Results of Tests
G2: Logical access to computer systems, programs, master data, client data, transaction data and parameters, including access by administrators to applications, databases, systems and networks, is restricted to authorised individuals via information security tools and techniques		
A. The identity of users is authenticated to the system through passwords or other authentication mechanisms. Policies relating to the use of passwords incorporate periodic password change, complexity, history of passwords and minimum length requirements.	**Observation** Observed that access to systems (e.g., network, application, databases, and operating systems) is restricted through the use of User IDs and passwords. **Inspection** Inspected password policy settings to ascertain the parameters were defined with minimum password length, password expiration, history and password complexity parameters that comply with the password configuration requirements defined in the Password Standards section of Morgan Stanley's Global Technology Policy.	No relevant deviations noted.
	Webstreme (Ausmaq Third party software) **Inspection** Inspected the Ausmaq ASAE3402 report regarding the effectiveness of internal controls related to Password access policy settings and system configuration.	No relevant deviations noted.

Control Activity	Service Auditor's Description of the Nature, Timing and Extent of Tests Applied to Controls	Results of Tests
B. The identity of users (remote) is authenticated to the network and communication software through passwords or other authentication mechanisms, in compliance with entity security policies.	**Observation** Observed that SecurID is being utilised to authenticate user access remotely, requiring a PIN and token code to be entered along with the Windows Domain credentials for the user. **Inspection** Inspected screenshots evidencing the system parameters and requirements of the SecurID system to ascertain that two-factor authentication is utilised for users to gain remote access.	No relevant deviations noted.
C. Procedures have been established for granting temporary access for technology personnel to the distributed production infrastructure environment (e.g., operating systems and databases) upon appropriate approval for incident handling or production management support Temporary access is managed through the TAM tool via a Temporary Access Privilege (TAP) request.	**Observation** Observed that the Temporary Access Management (TAM) tool includes documentation of approvals, access requested/granted and the duration for which the access is requested. Also, noted that the role was granted and revoked once the assigned time had elapsed. **Inspection** For a selection of users granted temporary access, inspected the TAP request and approval to ascertain the request had the required level of documentation to support the request (e.g., ServiceNow Ticket) and was approved by the appropriate resource owner based on their assigned job responsibility.	No relevant deviations noted.

Control Activity	Service Auditor's Description of the Nature, Timing and Extent of Tests Applied to Controls	Results of Tests
D. Network access for new employees is granted automatically once HR approves the access within HR system or when requested by the business unit Administrator through a ticket with approval of the hiring manager. For terminations, upon HR updating a termination flag and date in the HR system, an automated process disables terminated user's accounts on their last day. In the case of a termination of employees, vendors or contractors who "pose risk" based on management's assessment, Human Resource/Contingent Labor Operations ("HR/CLO") personnel use the Immediate Access Disablement ("IMAD") tool to immediately disable employee's access.	**Inspection** For a selection of new hires, noted through inspection of approval forms that their access to the Morgan Stanley network and applications was approved by the hiring manager. **Inspection** For a selection of terminated employees, noted through inspection of supporting documentation that upon HR updating a termination flag within the HR system, users' accounts in Windows Active Directory, UNIX, SecurID and TSS are disabled automatically. Further, noted through inspection of Active Directory configuration settings that terminated user was removed from the network. **Observation** Through observation conducted with the ("HR/CLO") personnel, ascertained that the IMAD tool is used for high-risk terminations and it disables access to the company network within 1 day. Further, observed that IMAD tool is designed to disable accounts in Windows Active Directory, UNIX, SecurID and TSS.	No relevant deviations noted.

Procedures have been established for granting, modifying and removing Webstreme user access based on authorisation. Access levels are determined by defined roles. Webstreme system privileged functions are restricted to authorized individuals.	**Webstreme (Ausmaq Third party software)** **Inspection** Inspected the Ausmaq ASAE3402 report regarding the effectiveness of internal controls related to new employee access approval to the applications/network and terminated employee timely access removal. **Observation** Through observation conducted with the platform owner, access is administered through Morgan Stanley's standard 'getaccess/' program with access restricted based on role and functions. Approval is by the user's manager and by an administrator. When a staff member changes roles or leaves the organisation, their profile will be updated in 'getaccess' and administrators will be notified immediately to terminate access. There is a small number of Webstreme users (12). Webstreme has only been operational for a few months and no changes have been required in relation to user access. **Inspection** Through inspection of the user's entitlements and the platform owners confirmation, noted that the Webstreme users' access was appropriate based on user's function and role. **Inspection** Inspected the Ausmaq ASAE3402 report regarding the effectiveness of internal controls related to employee restricted access to privileged functions. **Observation** Through observation conducted with the platform owner, privileged access is granted to Webstreme by authorised system administrators. **Inspection** Inspected the Ausmaq ASAE3402 report regarding the effectiveness of internal controls related to application users	No relevant deviations noted.

Control Activity	Service Auditor's Description of the Nature, Timing and Extent of Tests Applied to Controls	Results of Tests
	access to determine whether access to privileged functions in the applications was restricted to authorized individuals. **Observation** Through observation conducted with the platform owner, the total population with administration access was confirmed as appropriate and access was based on user's job function and role.	
G3: Segregation of incompatible duties is defined, implemented and enforced by logical security controls in accordance with job roles		
A. Privileged access to the network and production databases and operating systems is restricted to IT Operations and Production Management personnel whose job functions require such access.	**Inspection** Inspected users assigned privileged access (i.e., administrator privileges) to the network (Windows Active Directory), to the mainframe, for a selection of Linux servers (i.e. root access) and to the Windows servers (i.e., Windows local admin), to ascertain the access was appropriate based on their assigned job responsibility within production management. **Inspection** For a selection of databases and Windows servers, inspected the listing of users with administrator access to ascertain the access was appropriate based on their assigned job responsibility within production.	No relevant deviations noted

Control Activity	Service Auditor's Description of the Nature, Timing and Extent of Tests Applied to Controls	Results of Tests
	Webstreme (Ausmaq Third party software) **Inspection** Inspected the Ausmaq ASAE3402 report regarding the effectiveness of internal controls related to • new staff and staff leavers at Ausmaq's third party IT infrastructure provider who have access to production databases to determine respectively whether access was established following management approval and that access was revoked in a timely manner. • individuals from Ausmaq and its third party IT infrastructure provider with access to production databases to determine whether access was restricted to authorised personnel • access to privileged operating system functions within Ausmaq and its third party IT infrastructure provider to determine whether that access was restricted to authorised Administrators and DBA's.	No relevant deviations noted.
B. Access to business applications is restricted to authorised personnel according to job function by function-specific security access and is controlled through User IDs and passwords. Application password settings comply with IT security policies and procedures. Additions, changes and removals of user access rights to applications are administered according to standardised procedures and monitored by the Technology and Information Risk Access Management group and/or application business owners.	**Inspection** Through inspection of password parameter settings ascertained that the in-scope applications adhere to IT password standards such as minimum length, complexity, history and expiration. **Inspection** For a selection of employees, noted through inspection of supporting evidence that their access to the designated applications is appropriate per their job responsibilities and has been approved by appropriate personnel. For a selection of transferred and terminated employees, noted through inspection of documentation that their access to applications that they no longer should have access to is disabled.	No relevant deviations noted.

Control Activity	Service Auditor's Description of the Nature, Timing and Extent of Tests Applied to Controls	Results of Tests
Morgan Stanley Access to Webstreme is restricted and additions, changes and removal of user access rights to Webstreme are administered according to standardised process. Refer to Section G2 above.	**Webstreme (Ausmaq Third party software)** **Inspection** Inspected the Ausmaq ASAE3402 report regarding the effectiveness of internal controls related to • the 'Password and Access policy' to determine whether mandatory and recommended password configuration settings and parameters were defined. • the password configuration parameters at the application and network layers (Active Directory) at Ausmaq to determine whether they were configured in accordance with the Policy. • the authorisation matrix outlining roles and responsibilities within Ausmaq to determine whether segregation of incompatible duties was enforced by the application at a functional level. • system generated lists of application users to determine whether the roles and responsibilities were reflected in the applications in accordance with the authorisation matrix for Ausmaq users.	No relevant deviations noted.
C. Application-level user access reviews are performed annually by the designated individuals via a centrally managed process for certain applications; any users who no longer require access are removed.	**Inspection** Through inspection of the entitlement review data and corresponding sign-offs and/or application business owners, ascertained that the application and business owners perform access reviews for user entitlements on in scope application systems on an annual basis.	No relevant deviations noted.

Control Activity	Service Auditor's Description of the Nature, Timing and Extent of Tests Applied to Controls	Results of Tests
	Webstreme (Ausmaq Third party software) **Inspection** Inspected the Ausmaq ASAE3402 report regarding the effectiveness of internal controls related to user access reviews across Webstreme and Ausmaq's internal network to determine whether the currency and appropriateness of user profiles was maintained. **Inspection** There is a small number of Webstreme users (12). Webstreme has only been operational for a few months and no changes have been required in relation to user access. Through inspection of the user's entitlements and the platform owners confirmation, noted that the Webstreme users' access was appropriate based on user's function and role.	No relevant deviations noted.
D. User access privileges (i.e. administrative access) are periodically reviewed by application owners to ensure access privileges remain appropriate.	**Observation** Observed that user access privileges review was completed for the period. **Inspection** Inspected total population with administrative access (i.e. admins, windows admins TSS, UNIX) whose entitlements were marked as "maintained" and confirmed that these were based on users job function and role.	No relevant deviations noted.

Control Activity	Service Auditor's Description of the Nature, Timing and Extent of Tests Applied to Controls	Results of Tests
	Webstreme (Ausmaq Third party software) **Inspection** Inspected the Ausmaq ASAE3402 report regarding the effectiveness of internal controls related to user administration access reviews across Webstreme and Ausmaq's internal network to determine whether the currency and appropriateness of user profiles was maintained and such reviews were performed periodically. Refer to Section G3.C above.	No relevant deviations noted.
E. The ability to make modifications to overall system security parameters, security roles, or security configuration over application systems, data structures, network and communication software, and systems software is limited to appropriate personnel.	**Observation** Observed that the ability to make modifications to system security parameters, security roles, or security configuration over application systems, data structures, network is limited to privilege users. **Inspection** Inspected total population of privilege users (i.e. Windows, Mainframe, Linux, Windows Servers, UNIX and TSS) to ascertain the access was appropriate based on their assigned job responsibility within production management and noted that they were limited to appropriate personnel. Refer to Sections G3.A, G3.B, G3.C and G3.D above.	No relevant deviations noted.
	Webstreme (Ausmaq Third party software) **Inspection** Inspected the Ausmaq ASAE3402 report regarding the effectiveness of internal controls related to application users to determine whether access to privileged functions in the applications was restricted to authorized individuals.	No relevant deviations noted.

Control Activity	Service Auditor's Description of the Nature, Timing and Extent of Tests Applied to Controls	Results of Tests
G4: IT Processing is authorised and scheduled appropriately and exceptions are identified and resolved in a timely manner		
A. Job submission and execution rights are limited to authorised persons and/or processes utilising automated scheduling tools.	**Observation** Production jobs for systems and application processing run by Autosys use an application-specific production ID. Through observation conducted with the application owners, ascertained that jobs are scheduled, monitored and reviewed using Autosys. **Inspection** Through inspection of Autosys settings, noted that batch jobs pertaining to in scope applications are run via application specific production IDs. **ISG Mainframe** **Observation** In the Mainframe environment, all the production jobs are scheduled using Submitor. All production jobs run under an application specific Production ID. Through observation conducted with the application owners, ascertained that jobs in the mainframe environment are scheduled using Submitor. **Inspection** Through inspection of Submitor settings, noted that production job submissions are done through production IDs in Submitor. Also noted that modification of jobs is restricted to appropriate production management personnel.	No relevant deviations noted.

Control Activity	Service Auditor's Description of the Nature, Timing and Extent of Tests Applied to Controls	Results of Tests
	Webstreme (Ausmaq Third party software) **Inspection** Inspected the Ausmaq ASAE3402 report regarding the effectiveness of internal controls related to • one implementation plan which was signed off by the manager of the Client Services team to determine whether there was approval provided for modifications to the job schedule. • the list of individuals with access to the job schedule to determine whether access was restricted to authorised individuals.	No relevant deviations noted.

Control Activity	Service Auditor's Description of the Nature, Timing and Extent of Tests Applied to Controls	Results of Tests
B. Critical components of the environment, including production databases, production application processes, network, backups, and hardware, are monitored and alerts transmitted to the appropriate individuals in the event of failure. Tickets are logged in the Service Now ticketing systems and are tracked to resolution. Weekly Incident Management Review Meetings (WIRM) are conducted by the Enterprise Command Center (ECC) to review firm wide technology incidents.	**Observation** Observed that critical components of the environment are monitored and alerts are transmitted to appropriate individuals in the event of a failure using automated tools. Observed that servers and jobs are automatically monitored and processing errors are corrected to ensure successful completion. **Inspection** For a selection of production incidents, obtained the ServiceNow tickets, and noted that the incidents are investigated, resolved and closed. For a selection of weekly Incident Management Review Meetings (WIRM), inspected meeting documentation minutes for users in attendance and review of incidents discussed. **ISM Mainframe** **Inspection** Through inspection of a sample of Submitor abends, noted that jobs were succesfully rerun or the incidents were escalated and tracked to resolution.	No relevant deviations noted.
	Webstreme (Ausmaq Third party software) **Inspection** Inspected the Ausmaq ASAE3402 report regarding the effectiveness of internal controls related to the logging and resolution of a sample of jobs to determine whether it was resolved in a timely manner.	No relevant deviations noted.

Control Activity	Service Auditor's Description of the Nature, Timing and Extent of Tests Applied to Controls	Results of Tests
G5: Appropriate measures, including firewalls and anti-virus software, are implemented to counter the threat from malicious electronic attack		
A. Firewalls Firewalls are implemented and have been configured to restrict unwanted and unauthorised access from external networks. Intrusion detection systems are utilised to monitor activity. Activity that requires further analysis is escalated to the Computer Emergency Response Team ("CERT").	**Observation** Observed that firewalls and intrusion detection systems are utilised with the IT environment. **Inspection** Inspected certain firewall configuration to ascertain it is operating in a fail secure mode (deny traffic unless it is specifically allowed). Inspected samples of incidents, inspected the corresponding tickets to ascertain monitoring and resolution by the CERT was performed.	No relevant deviations noted.

Control Activity	Service Auditor's Description of the Nature, Timing and Extent of Tests Applied to Controls	Results of Tests
	Webstreme (Ausmaq Third party software) **Inspection** Inspected the Ausmaq ASAE3402 report regarding the effectiveness of internal controls related to • users with access to the firewall rules to determine whether there was restriction of access to authorised personnel. • firewall configurations to determine whether firewalls were in place and actively configured. • infrastructure checklists and firewall monitoring check sheets to determine whether firewall monitoring was performed. • topology diagrams to determine whether controls were in place to restrict access to authorised IP addresses. • a sample of monthly infrastructure checklists and antivirus detection and correction check sheets to determine whether they were completed and included monitoring of the availability of the connection, antivirus monitoring was performed on a monthly basis and whether detected virus issues were tracked and addressed. • a sample of monthly SLA reports provided by the third party IT infrastructure providers to Ausmaq reporting on the status of network and ativirus activities in the month to determine whether monitoring occurred. • whether Antivirus software was in place at Ausmaq and its third party IT infrastructure provider and inspected antivirus settings to determine whether daily updates occurred.	No relevant deviations noted.

Control Activity	Service Auditor's Description of the Nature, Timing and Extent of Tests Applied to Controls	Results of Tests
G6: The physical IT equipment is maintained in a controlled environment		
A. Data centres have independent air conditioning systems, humidity and temperature controls, smoke and fire detection and notification systems and a Halon fire suppression system. Data centres are equipped with surge protectors, uninterruptible power supplies and generators to protect IT resources in the event of a power disruption. Environmental control systems in each data centre are monitored through local and centralised monitoring stations.	**Observation** Observed the in-scope data centres, and noted the existence of independent air conditioning systems, humidity and temperature controls, smoke and fire detection and notification systems and a halon fire suppression system. Observed the data centres and noted the existence of power supplies and generators to protect IT resources in the event of a power disruption. **Observation** Observed monitoring stations and confirmed with the Data Centre Operations that data centres are monitored continuously.	No relevant deviations noted.
	Webstreme (Ausmaq Third party software) **Inspection** Inspected the Ausmaq ASAE3402 report regarding the effectiveness of internal controls related to Ausmaq's data centre and disaster recovery site to determine whether physical IT equipment was secure and that environmental controls were in place.	No relevant deviations noted.

Control Activity	Service Auditor's Description of the Nature, Timing and Extent of Tests Applied to Controls	Results of Tests
G7: Development and implementation of new systems, applications and software, and changes to existing systems, applications and software, are authorised, tested, approved, implemented and documented.		
A. The object turnover process is synchronised with the storage of source version in a repository to ensure that the current production source can be identified. In addition, prior versions are stored in a repository, in case a scenario exists where a version rollback is necessary.	**ISG Distributed** **Observation** Observed that current and prior versions of source codes are stored in a repository where Perforce and Git allows simultaneous changes of files with the ability to merge such changes into one final version. **ISG Mainframe** **Observation** Observed that the Change Management (CM) application provides a source code repository and turnover mechanism to production code libraries.	No relevant deviations noted.

Control Activity	Service Auditor's Description of the Nature, Timing and Extent of Tests Applied to Controls	Results of Tests
B. A source control system or process is in place that supports code locking and identifies or prevents code collisions (i.e. parallel programming). Code collisions are appropriately resolved prior to further development in the event that two or more developers are working on the same piece of code.	**ISG Distributed** **Observation** Observed the source code control system and noted that developers are able to "check in" and "check-out" code while making changes. The system also identifies and prevents code collisions. **Observation** Observed the source code control system and noted systems are configured to locked down code and prevent changes when it is "checked out" by a developer. **ISG Mainframe** **Observation** Observed that the Change Management (CM) application provides a source code repository and turnover mechanism to production code libraries. **Observation** Observed the source code control system and noted systems are configured to locked down code and prevent changes when it is being edited by a developer.	No relevant deviations noted.

Control Activity	Service Auditor's Description of the Nature, Timing and Extent of Tests Applied to Controls	Results of Tests
C. Business Unit and/or IT staff, as appropriate, sign off on the testing to confirm that the change to an application or database object is functioning as intended. The business risks and impact of proposed application systems, databases, network and communication software, and systems software changes is assessed and reviewed by management before implementation. The results of this assessment is used when designing, staffing, and scheduling migration and/or	**Inspection** For a selection of application, database and infrastructure changes, inspected a sample of Technology Change Management ('TCM') tickets for the ISG Distributed and ISG Mainframe applications and evidenced that: 1. Severity of change is documented along with risk assessment 2. Change was moved in production in the appropriate timeframe 3. Testing was successfully performed over change 4. Change was approved by Appropriate Personnel 5. All approvals were received prior to turnover date	No relevant deviations noted.

Control Activity	Service Auditor's Description of the Nature, Timing and Extent of Tests Applied to Controls	Results of Tests
conversion of information technology, in order to minimize disruptions to operations.	**Webstreme (Ausmaq Third party software)** **Inspection** Inspected the Ausmaq ASAE3402 report regarding the effectiveness of internal controls related to • a sample of hot fixes and data fixes at Ausmaq to determine whether they followed the change management process. • a sample of infrastructure changes at Ausmaq's third party IT infrastructure provider to determine whether they followed the change management process. • the development, test and production environments at Ausmaq to determine whether physical and logical segregation of environments exists. • a sample of monthly production modification audit reports to determine whether this was reviewed by the Head of IT to enforce segregation in change requests. • the development, test and production environments at Ausmaq to determine whether physical and logical segregation of environments exists.	No relevant deviations noted.
D. Emergency changes within the distributed environment can be moved into production without an approved TCM. These changes are logged and tracked in the Change Management Reporting System ("CMRS"). Application owners are required to review and sign-off on each emergency change no later than 14 days from the date of occurrence. Monitoring of emergency changes is performed weekly. The Change Management Working Group ("CMWG")	**Inspection** For a selection of emergency changes in the distributed environment, obtained and inspected the change documentation to ascertain the changes were documented and approved in CMRS within 14 days of being implemented into production. For a sample of weeks, inspected Change Management Working Group ("CMWG") meeting minutes for log of attendees, meeting focus areas, agenda topics, and emergency changes reviewed to ascertain managements monitoring of the use of emergency changes.	No relevant deviations noted.

Control Activity	Service Auditor's Description of the Nature, Timing and Extent of Tests Applied to Controls	Results of Tests
provides monitoring reports to individual CIOs and their delegated representatives to provide the root cause of the use of emergency changes.	**Webstreme (Ausmaq Third party software)** **Inspection** Inspected the Ausmaq ASAE3402 report regarding the effectiveness of internal controls related to the formal change management policy for both Ausmaq and its third party IT infrastructure provider to determine the existence of change management procedures.	No relevant deviations noted.
E. Emergency changes in the ISG mainframe environment follow the standard change management process where they are authorised by an appropriate manager prior to turnover. For emergency changes where approvals cannot be obtained prior to turnover, appropriate IT management approvals are obtained after the fact in a timely manner.	**Observation** Observed that in the mainframe environment, emergency changes follows the same process as non emergency changes.	No relevant deviations noted.

Control Activity	Service Auditor's Description of the Nature, Timing and Extent of Tests Applied to Controls	Results of Tests
G8: Data Migration or modification is authorised, tested and, once performed, reconciled back to the source data		
A. Urgent data fixes for Webstreme are updated via specifically written programs that are executed by DBA's and pre-approved.	**Webstreme (Ausmaq Third party software)** **Inspection** Inspected the Ausmaq ASAE3402 report regarding the effectiveness of internal controls related to • the formal project documentation for one scheduled release which included data migration within the reporting period to determine whether appropriate change management procedures were followed. • a sample of data modifications to determine whether they were approved in line with the change management process.	No relevant deviations noted.
G9: Data and systems are backed up regularly offsite and regularly tested for recoverability on a periodic basis		
A. Backups of databases, datasets, application programs, system software and files are executed through an automated backup tool according to Company policy. Throughout the week, incremental backups are performed daily and full backups are performed weekly. The backup process is monitored and errors are resolved by the production support team. Backup tapes are taken off-site weekly to offsite storage facility.	**Observation** Performed an observation with Enterprise Infrastructure personnel to ascertain that an automated tool is used to perform daily / weekly backups according to Company policy. **Inspected** For a selection of weeks, inspected documentation to ascertain that weekly or daily backup's processes were monitored and that errors (if any within our sample) were resolved by the production support team. For a selection of weeks, inspected documentation to ascertain that weekly backup tapes were taken offsite.	No relevant deviations noted.

Control Activity	Service Auditor's Description of the Nature, Timing and Extent of Tests Applied to Controls	Results of Tests
	Webstreme (Ausmaq Third party software) **Inspection** Inspected the Ausmaq ASAE3402 report regarding the effectiveness of internal controls related to • the existence of a back-up schedule to determine whether backups were performed on a daily basis. • a sample of backups performed at third party IT infrastructure provider to determine whether there was successful completion and resolution of failed backups. • the third party IT infrastructure provider whether automatic production data replication was in place and inspected evidence of the replication tool in place. • a sample of incidents at Ausmaq's third party IT infrastructure provider to determine whether they were monitored and resolved in a timely manner.	No relevant deviations noted.
G10: IT Hardware and software issues are monitored and resolved in a timely manner		
A. The problem management process ensures that the production environment, including hardware, network, backups, and database	Refer to Section G4 above.	No relevant deviations noted.

Control Activity	Service Auditor's Description of the Nature, Timing and Extent of Tests Applied to Controls	Results of Tests
problems are captured, tracked and addressed.	**Webstreme (Ausmaq Third party software)** **Inspection** Inspected the Ausmaq ASAE3402 report regarding the effectiveness of internal controls related to • whether incident management policies and procedures were in place at the third party IT infrastructure vendor. • a sample of hot fixes and data fixes at Ausmaq to determine whether they were resolved in a timely manner. • a sample of 25 incidents at Ausmaq's third party IT infrastructure provider to determine whether they were resolved in a timely manner. • a sample of production support fortnightly meetings to determine whether hardware/software issues were monitored. • a sample of monthly SLA reports provided by Ausmaq's third party IT infrastructure providers reporting on the status of incidents in the month to determine whether monitoring occurred.	No relevant deviations noted.
G11: Business and information systems recovery plans are documented, approved, tested and maintained		
A. Critical application data is mirrored to an alternate data centre on a real-time basis. Critical corporate data is replicated through various technologies to alternate backup systems and locations. Business and information recovery plans are documented, approved, tested and maintained. Each Business Unit maintains	**Observation** Observed that Disaster Recovery Tests are performed annually to ensure business and information recovery plans are documented, approved, tested and maintained. **Inspection** For a selection of TRPs noted that the plans are inclusive of the following areas: System Details, Failover Checks, Data Recovery and Ready for Business (RFB) Check.	No relevant deviations noted.

Control Activity	Service Auditor's Description of the Nature, Timing and Extent of Tests Applied to Controls	Results of Tests
and updates documented Business Continuity Plans on a semi-annual basis. Disaster Recovery Tests are conducted at least once a calendar year for all critical applications. Testing on critical applications is performed at least annually. The Technical Recovery Plans (TRP) contains detailed information for all of the critical business systems. Server information, failover information and contacts are updated regularly within TPR.	**Webstreme (Ausmaq Third party software)** **Inspection** Inspected the Ausmaq ASAE3402 report regarding the effectiveness of internal controls related to • the Business Continuity and Disaster Recovery plans at Ausmaq to determine whether contingency procedures were planned. • the Business Continuity and Disaster Recovery plans to determine whether the plans were approved by appropriate personnel. • test results to determine whether Business Continuity and Disaster Recovery plans were tested. It was noted by the Service Auditor that the Disaster Recovery test results for one in-scope application was to be tested outside of the audit period. Through the platform owners confirmation, it was observed that Business Continuity testing was performed with Ausmaq as part of the setup of the Webstreme application in May 2018.	No relevant deviations noted.
G12: Information technology services provided to clients are approved, managed and performance thresholds met in accordance with the requirements of the client agreement		
Not Applicable – no IT services are provided to customers.		

Control Activity	Service Auditor's Description of the Nature, Timing and Extent of Tests Applied to Controls	Results of Tests
G13: Appointment of sub-service organisations, including those providing IT services, are approved, sub-service organisations are managed in accordance with the requirements of the client agreement and their activities are adequately monitored		
Webstreme (Ausmaq Third party software) A. Contracts are in place for 3rd party service providers. SLA's are monitored and reported to management monthly. Controls operating at the third party IT application provider are monitored on a periodic basis.	**Webstreme (Ausmaq Third party software)** **Inspection** Inspected the Ausmaq ASAE3402 report regarding the effectiveness of internal controls related to SLA documents to determine whether services were agreed between Ausmaq and their IT service provider. Inspected the Ausmaq ASAE3402 report regarding the effectiveness of internal controls related to a sample of • vendor reports from Ausmaq's third party IT infrastructure providers to determine whether reporting and monitoring of SLA attainment took place. • quarterly compliance meetings to determine whether there is monitoring of control compliance by the third party IT infrastructure provider. **Observation** Observed though enquiry that Morgan Stanley hold regular meetings with Ausmaq.	No relevant deviations noted.

Appendix 1 – List of sub-custodians

Country	Bank Name
Abu Dhabi & Dubai	HSBC Bank Middle East Limited
Argentina	Industrial and Commercial Bank of China (Argentina) S.A.
Australia – Fixed Income	Citigroup Pty Limited
Australia - Equity	The Hongkong and Shanghai Banking Corporation Limited (Sydney)
Austria	UniCredit Bank Austria AG (Vienna)
Bahrain	HSBC Middle East Bank Limited (managed by UAE team
Belgium	BNP Paribas Securities Services S.A
Brazil	Itau Unibanco S.A.
Bulgaria	Citibank Europe plc., Bulgaria Branch
Canada	Royal Bank of Canada (Toronto)
Chile	Banco de Chile
China	HSBC Bank (China) Company Limited
Colombia	Cititrust S.A.
Croatia	SPLITSKA BANKA Societe Generale Group
Cyprus	BNP Paribas Securities Services (Athens)
Czech Republic	Deutsche Bank AG Filiale Prag
Denmark	Skandinaviska Enskilda Banken AB (publ), Copenhagen Branch
Egypt	Citibank, N.A
Estonia	Swedbank AS (Tallinn)
Euroclear	Euroclear Bank S.A.
Finland	Skandinaviska Enskilda Banken AB (publ), Helsinki Branch
France (Equity)	BNP Paribas Securities Services S.A.
France (Fixed Income)	BNP Paribas Securities Services S.A.
Germany	Morgan Stanley Bank AG (Frankfurt)
Greece	BNP Paribas Securities Services
Hong Kong (Eq Physicals and Fixed Income)	Standard Chartered Bank (Hong Kong) Limited
Hong Kong (Scripless Equity)	Morgan Stanley Hong Kong Securities Limited
Hungary	Citibank Europe plc Hungarian Branch Office
Iceland	Landsbankinn hf
India	Citibank N.A.
Indonesia	The Hongkong and Shanghai Banking Corporation Limited (Jakarta)
Ireland	Morgan Stanley Securities Limited (UK)
Israel	Bank Leumi
Italy	Citibank, N.A. (Milan)
Japan (Activist business)	The Hongkong and Shanghai Banking Corporation Limited (Tokyo)
Japan (Government Bonds)	The Bank of TokyoMitsubishi UFJ Ltd
Japan	Morgan Stanley MUFG Securities Co., Ltd
Kazakhstan	JSC Citibank Kazakhstan
Kenya	CFC Stanbic Bank Ltd
Kuwait	HSBC Bank Middle East Limited
Latvia	AS SEB Banka, Riga

Country	Bank Name
Lithuania	SEB Banks
Luxembourg	BNP Paribas Securities Services S.A.
Malaysia	HSBC Bank Malaysia Berhad
Mexico	Banco Nacional de Mexico, S.A (Banamex) (Mexico City)
Morocco	Citibank Morocco
Netherlands	BNP Paribas Securities Services S.A.
New Zealand	The Hongkong and Shanghai Banking Corporation Limited (New Zealand)
Nigeria	Stanbic IBTC Bank plc
Norway	Skandinaviska Enskilda Banken AB (publ), Oslo Branch
Oman	HSBC Bank Oman SAOG
Pakistan	Standard Chartered Bank (Pakistan) Limited
Peru	Citibank del Peru S.A.
Philippines	The Hongkong and Shanghai Banking Corporation Limited (Manila
Poland	Bank Polska Kasa Opieki S.A
Portugal	BNP Paribas Securities Services S.A.
Qatar	HSBC Bank Middle East Limited
Romania	Citibank Europe plc Dublin Romania branch
Russia	ZAO Citibank
Saudi Arabia	Morgan Stanley Saudi Arabia
Saudi Arabia	The Saudi British Bank (SABB)
Serbia	Unicredit Bank Serbia JSB
Singapore	Standard Chartered Bank, Singapore Branch
Slovak Republic	Citibank Europe Plc. Pobocka zahranicnej banky
Slovenia	SKB Banka d.d. Ljubljana
South Africa	Standard Bank of South Africa (Johannesburg)
South Africa	Citibank NA
South Korea	The Hongkong and Shanghai Banking Corporation Limited
Spain (Equity	BNP Paribas Securities Services (Madrid)
Spain (Fixed Income)	Citibank International Limited,
Sri Lanka	The Hongkong and Shanghai Banking Corporation Limited
Sweden	Skandinaviska Enskilda Banken AB (publ.)
Switzerland	Bank Morgan Stanley AG
Taiwan	HSBC Bank (Taiwan) Limited
Thailand	The Hongkong and Shanghai Banking Corporation Limited (Bangkok)
Turkey	Citibank, A.S.
Ukraine	PJSC "Ukrsotsbank"
United Kingdom	Morgan Stanley &Co. International plc
United States (Equity & Fixed Income)	Morgan Stanley & Co. LLC (NY)
United States (Government Securities)	Bank of New York (NY)
Vietnam	HSBC Bank (Vietnam) Ltd.