Morgan Stanley

Report on the Internal Controls for Private Wealth Management Custody Services of Morgan Stanley Wealth Management Australia Pty Ltd

ASAE 3402 report for the period 1 July 2018 to 30 June 2019

Table of contents

Section I:
Executive Summary

Section I: Executive Summary

Overview

This report has been prepared to provide clients (or "users") of Morgan Stanley Wealth Management Australia Pty Ltd ("MSWM") 's Private Wealth Management ("PWM") custody services with a description of its system of internal controls. The system, or internal control environment, is an essential component of an organisation's governance structure. The objectives of an internal control system are 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 valid. The management of MSWM have established and maintained an internal control system that monitors compliance with established policies and procedures.

This report will be provided to relevant users and their auditors, who have a sufficient understanding to consider it, along with other information including information about controls operated by users themselves, so they may assess the risks of material misstatements of users' financial reports. It may be provided to others as authorised by MSWM and Deloitte Touche Tohmatsu ("Deloitte").

Scope

The scope of this report includes the description of MSWM's PWM custody services throughout the period from 1 July 2018 to 30 June 2019 (the description), and on the design and operating effectiveness of controls related to the control objectives stated in the description.

This report has been prepared in accordance with Australian Standard on Assurance Engagements 3402 *Assurance Reports on Controls at a Service Organisation* ("ASAE 3402"). ASAE 3402 conforms with the International Standard for Assurance Engagements 3402 *Assurance Reports on Controls at a Service Organization* ("ISAE 3402").

The control objectives in this report are directly referenced from Guidance Statement GS 007 *Audit Implications of the Use of Service Organisations for Investment Management Services* ("GS 007" or "the Guidance Statement"), issued by the Auditing and Assurance Standards Board in Australia.

The specific controls set out in Section VI of the report have been designed to achieve each of the control objectives. The controls have been in place throughout the period from 1 July 2018 to 30 June 2019 unless otherwise indicated.

Specifically excluded from the scope of the report are complementary user entity controls, that is, controls assumed to be implemented by customers for stated control objectives to be met. Also excluded from the scope are other services provided by us not described in the description of the system and control activities.

This report includes controls (carve in) operated by internal affiliates of MSWM who perform functions to support the custody services MSWM's provides to its PWM clients.

This report does not include (carved out) controls at external sub-service organisations of MSWM. The effectiveness of controls performed by users and their service providers should also be considered as part of the overall system of controls.

Summary of results

Below is a summary of the service auditor's results and conclusions, by control objective. This summary of results does not provide all details relevant for users and their auditors and should be read in conjunction with the entire report. The details of the specific controls tested, and the nature, timing and extent of those tests, are listed in Section VI.

Control Objective	Number of controls effectively designed and operated	Number of controls per control objective	Results	Conclusion (in all material respects)
A.1 New accounts are set up completely and accurately in accordance with client agreements and any applicable regulations.	2	2	No deviations noted	Control objective met
A.2 Complete and authorised client agreements are established prior to initiating custody activity.	1	1	No deviations noted	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	No deviations noted	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	No deviations noted	Control objective met
A.5 Corporate actions are identified, actioned, processed and recorded on a timely basis.	4	4	No deviations noted	Control objective met
A.6 Cash receipts and payments are authorised, processed and recorded completely, accurately and on a timely basis	2	2	No deviations noted	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	N/A – MSWM does not provide its PWM clients securities lending services	N/A
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	N/A – MSWM does not provide its PWM clients loan services	N/A
A.9 Collateral is completely and accurately invested in accordance with the lender's agreement.	N/A	N/A	N/A – MSWM does not provide obtain collateral from its PWM clients	N/A
A.10 Accounts are administered in accordance with client agreements and any applicable regulations.	3	3	No deviations noted	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	No deviations noted	Control objective met
A.12 Investment income and related tax reclaims are collected and recorded accurately and on a timely basis.	4	4	No deviations noted	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	No deviations noted	Control objective met
A.14 Assets held (including investments held with depositories, cash and physically held assets) are safeguarded from loss,	4	4	No deviations noted	Control objective met

Control Objective	Number of controls effectively designed and operated	Number of controls per control objective	Results	Conclusion (in all material respects)
misappropriation and unauthorised use.				
A.15 Assets held are appropriately registered and client money is segregated.	1	1	No deviations noted	Control objective met
A.16 Transaction errors are rectified promptly.	3	3	No deviations noted	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	No deviations noted	Control objective met
A.18 Client reporting in respect of client asset holdings is complete and accurate and provided within required timescales.	3	3	No deviations noted	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	N/A – MSWM does not provide its PWM clients securities lending services	N/A
G.1 Physical access to computer networks, equipment, storage media and program documentation is restricted to authorised individuals.	1	1	No deviations noted	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	No deviations noted	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	No deviations noted	Control objective met
G.4 IT processing is authorised and scheduled appropriately and deviations are identified and resolved in a timely manner.	2	2	No deviations noted	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	No deviations noted	Control objective met
G.6 The physical IT equipment is maintained in a controlled environment.	1	1	No deviations noted	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.	6	7	Deviations noted. Changes could be made to database resources after the All Approved Date and prior to release.	Control objective met

Control Objective	Number of controls effectively designed and operated	Number of controls per control objective	Results	Conclusion (in all material respects)
			A mitigating control was identified and tested, refer to G.7.E.	
G.8 Data migration or modification is authorised, tested and, once performed, reconciled back to the source data.	1	1	No deviations noted	Control objective met
G.9 Data and systems are backed up regularly offsite and regularly tested for recoverability on a periodic basis.	1	1	No deviations noted	Control objective met
G.10 IT hardware and software issues are monitored and resolved in a timely manner.	1	1	No deviations noted	Control objective met
G.11 Business and information systems recovery plans are documented, approved, tested and maintained.	1	1	No deviations noted	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 – no IT services are provided to clients.	N/A
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	No deviations noted	Control objective met

Section II:
Statement by the Service Organisation

Section II: Statement by Morgan Stanley Wealth Management Australia Pty Ltd

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

(a) The accompanying description in Section III which includes control objectives and control activities included in Section V fairly presents the PWM custody services throughout the period 1 July 2018 to 30 June 2019. 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 MSWM's system during the period 1 July 2018 to 30 June 2019.

i. 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 July 2018 to 30 June 2019. 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 July 2018 to 30 June 2019.

Signed on behalf of Management of MSWM.

Astrid Ullmann

Chief Operating Officer
Morgan Stanley Wealth Management

22 November 2019

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

Section III: 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 and Deloitte. The information in this report is prepared with reference to the guidance in Standard on Assurance Engagements ASAE 3402 *Assurance Reports on Controls at a Service Organisation May 2017*, 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).

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 MSWM

MSWM's immediate parent undertaking is Morgan Stanley Domestic Holdings Inc. MSWM's ultimate parent undertaking and controlling entity is Morgan Stanley & Co LLC ("MSCL") which, together with MSWM and Morgan Stanley's other subsidiary undertakings, form the Morgan Stanley Group. MSWM 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.

MSWM 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 Corporations (Repeal and Transitional) Instrument 2016/396.

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. 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 PWM custody services provided to MSWM PWM clients. This report is intended to provide an understanding of the description 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, India and the United States.
The report covers controls over the following areas with regard to MSWM accounts on the PWM platform:

- Account set-up and account modification
  - Open new accounts, maintain existing accounts and update client account information, as required, and in accordance with internal processes
- Trading, trade support and settlement
  - Execution, booking and settlement of all trades executed through the MSIP platform
- Cash management
  - Manage deposits and payments for all clients on the PWM platform
- Security transfers
  - Process incoming and outgoing security transfers
- Errors handling
  - Manage all errors in a timely manner and in accordance within defined Risk procedures
- Investment income and corporate income
  - Process all investment related income directly to the client account
- Reconciliation
  - Reconcile all positions and ensure all positions are accurately reflected on client accounts
- Custody
  - Maintain client assets through agent Custodians and Sub-Custodians in different countries and monitor the network of Custodians through an ongoing review process client reporting

    - Report all positions held in Custody and provide monthly reporting to all clients on the PWM platform
- Information system security
    - Maintain information security to the highest standards to protect business information from modification and disruption
- Information system operations
    - Internal systems used to process day-to-day transactions on the PWM platform
- Application development and maintenance, and
    - Develop and maintain internal applications to ensure systems are up-to-date and software product development is maintained effectively.
- Business continuity management.
    - Global Business Continuity management plan that ensures the Firm is prepared in advance for potential business-impacting incidents

For the above mentioned areas, the operational and technology controls are the responsibility of MSWM however many are operated by MSWM internal affiliates. Controls at internal affiliates MSIP, MSCL and Morgan Stanley Institutional Securities Group (MSISG) are included in scope of this report to the extent they relate to custody services provided to MSWM PWM clients. Refer to Section VI for these relevant controls.

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.

Some MSWM clients have the custody service provided outside of Morgan Stanley by third party service providers. This occurs in some circumstances for specific products (e.g. hedge funds). For these client relationships, the activities handled by third party service providers are outside the scope of this report.

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 the Morgan Stanley's PWM 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 control objectives and related controls activities are described in more detail in Section VI. In determining the controls and control objectives we took into account the following criteria:

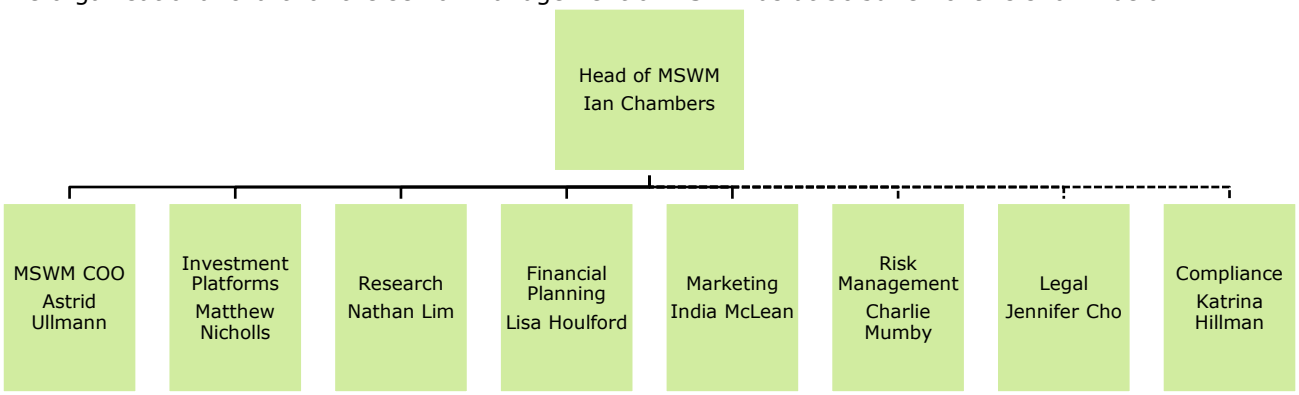
- The risks that threatened achievement of the control objectives stated in the description were identified;
- The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved; and
- The description 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 30 June 2019 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
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.

MSWM has developed departmental responsibilities and reporting structures to ensure that there is adequate segregation of functions and duties throughout the business.

Key functions and duties are appropriately segregated as follows

- The front office (trade execution and processing) function must be segregated from the back-office function (setting up new client accounts, reconciliation process and financial reporting);
- Compliance, legal and audit are separate functions and provides compliance and monitoring oversight across the business.

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.

Additionally, MSWM has the following in place to reduce risk:

- Insurance Policies - MSMW maintains adequate levels of insurance and is review on a yearly basis.
- Business Continuity Plans - Business continuity involves infrastructure solutions that have been implemented to provide full application redundancy whilst simplifying business continuity arrangements so that they are either initiated automatically or can be actioned by staff in a timely manner.
- Disaster Recovery Plan - MSWM has disaster recovery plans in place. Testing is done annually for work area recovery (WAR) site and plans are updated annually.

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.

MSWM's policies and procedures are subject an annual review by the Executive Committee, MSWM BOARD, Audit Committee and Legal and Compliance Division (LCD).

These included:

- Compliance Monitoring – MSWM's compliance team performs the independent checking and observing of each business or function's adherence to relevant rules and/or policies and procedures (e.g. through sample-based re-performance, review of possible exceptions flagged via detection scenarios, and trends analysis of first-line compliance activities, or through other methods)
- Conflict of interest – MSWM manages conflicts of interest via the implementation of internal control policies, processes and procedures, including standards of conduct; disclosure; avoidance; and monitoring.
- Breach reporting – MSWM maintains a breach register for internal and external breaches. This is monitored and reported to the Board.

3.8 Complimentary User Entity Controls

MSWM's services were designed with the assumption that certain controls would be placed in operation at user entities. This section describes controls that should be in operation at user entities to complement the controls at MSWM.

Specifically, controls should be established to validate that:

- User entity instructions and information provided to MSWM should be in accordance with the provisions of the client agreement or other applicable governing agreements or documents in effect between MSWM and the client
- The user entity should have sufficient controls to ensure that proper instructions are authorised, timely and in accordance with regulatory requirements. User entities should have effective controls over the authorisation, periodic review and removal of access rights for their staff to access systems.
- User entities should provide proper instructions and information to MSWM using data transmission delivery methods in accordance with MSWM security standards. Instructions and information provided to MSWM using methods not in accordance with the security standards may be less secure. The user entity should have sufficient controls to ensure that the set-up of new accounts on applicable systems or changes to existing accounts are authorised, approved and implemented.
- User entities should provide MSWM with timely written notification regarding changes to those individuals authorised to instruct on behalf of client activities.
- User entities should periodically review standing instructions provided to MSWM
- User entities should establish, monitor and maintain effective controls over physical and logical access to their computer systems via PCs at client locations.
- User entities should perform a timely review of reports provided for holdings and cash balances and related activity and provide written notice of any discrepancies.
- User entities should provide timely tax information to MSWM to ensure the efficient completion of year-end reporting

This list does not represent a comprehensive set of all the controls to be employed by user entities. Other controls may be required at user entities, depending upon each individual circumstance.

4 Operations and infrastructure support model – affiliates 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
- 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 (MSISG) as outlined below:

- MSISG handles for MSWM's 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
- MSISG 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.

Key Third Party / External Subservice Organisations

MSWM uses the services of third-party service providers in some operations with Service Level agreements in place. Monitoring of service providers is overseen by Management, with compliance undertaking periodic monitoring to ensure that counterparties are complying with reporting and other contractual obligations.

MSWMs key external subservice provider relevant to supporting custody services for MSWM PWM clients is Ausmaq, in the provision of investor statement reporting. This report does not include controls at Ausmaq or any other external sub-service organisation.

The effectiveness of controls performed by users and their service providers should also be considered as part of the overall system of controls.

5 IT systems

5.1 Network and Infrastructure

MSWM PWM utilises 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".

5.3 BCM/DRP

Morgan Stanley maintains global programs for business continuity management and technology disaster recovery that facilitate activities designed to protect the Firm during a business continuity event. A business continuity event is an interruption with potential impact to normal business activity of the Firm's people, operations, technology, suppliers, and/or facilities.

The business continuity program's core functions are business continuity planning (with associated testing) and crisis management. The Firm has dedicated Business Continuity Management staff responsible for coordination of the program governed by the Business Continuity Governance Committee and a Risk Oversight Committee. In addition, a Committee of the Board of Directors (the "Board Committee") and senior management oversee the program. BCM reports to the Board Committee at least annually on the status of program components such as business continuity events and business continuity testing results.

BCM facilitates the exchange of information within the Firm during an incident. BCM works with partners in Technology, Security, and Corporate Services to assess incidents for the level of impact to businesses and, as appropriate, escalate them accordingly. BCM provides 24/7 global coverage to monitor and manage incidents.

5.4 In Scope Applications

The following applications are applicable to the delivery of custody services to MSWM PWM clients.

Application	Description
AQUA	US Aqua coverage includes but is not limited to (1) daily SEC 15c3-3 customer reserve; (2) daily and monthly SEC 15c3-1 securities haircuts; (3) monthly SEC 15c3-1 FOCUS reporting. UK Aqua calculates the daily client money lockup required by the FCA.
CashForecasting	CashForecasting automates the process of forecasting cash requirements in various currencies and generating fx spot, money market, fiduciary and bank deposit orders, as appropriate and electronically transmit to the relevant execution and processing systems.
IWM Client Management	Strategic project for IWM to create a centralized client data repository.
FC3	FC3 is a Client trade confirmation system that delivers trade confirmations. Confirms are delivered to clients based in incoming trade messages matching rules that are managed by client service in Operations. This platform is responsible for intra-day confirmation of client trading to custodians and clients globally, supporting both industry standard and client specific formats to meet internal, external and regulatory requirements.
Intellimatch (Ops Control Apps)	Intellimatch is a generic reconciliation system that receives data from a variety of both internal and external data sources to carry out reconciliations for multiple internal customers. Data from the Intellimatch system is downloaded to a number of risk tracking and management reporting functions.
QWEST	QWEST (Query Workflow Exceptions Services Technology) is an Enterprise-wide application that consolidates information from many underlying data sources into one portal.
SAFE Global Settlements	SAFE is Morgan Stanley's in-house settlement system. SAFE ensures that the contract agreed between two trading parties is fulfilled. In its simplest form, SAFE facilitates the transfer of securities and cash as per the agreement on the trade contract and notes exceptions.
Scorpio	Covers the Scorpio application for calculation of entitlements arising from corporate actions and dividends and processing elections of those entitlements
STP Workstation	PWM STP Workstation is a PWM Proprietary order entry and order management system. It supports Equities, Options, OTC's, Mutual Funds and Fixed Income products. It performs order capture, pre-trade checks, execution and client side booking support.
T2	T2 is a trade capture and lifecycle management system for Equity OTC derivative trades and positions and their hedges. For listed equity derivatives and cash equities, it also provides the ability to move positions between internal firm accounts and to capture off-exchange trades with external brokers.
LiveWire	LiveWire GUI enables maintenance & tracking of deals, rates and clients in Wire, track charges in Global Billing System and create overrides in RBC system.
ASRV	This is the renovated platform for Asset Services applications.
Presto	Presto is a strategic solution to automate critical manual processes and replace the EUCs and tactical applications in the Firm. Presto is best fit for: 1) Control reporting - reports/alerts to facilitate users to perform control/monitoring functions 2) Data integration - data exchange between MS and external system in a variety of data formats 3) Data integrity check - detect data integrity issue before further user or downstream processing.
Client Suitability Engine (CSE)	Web application and middle tier services, that will be used for assessing the client Suitability and Eligibility - for pre and post trade checks (PRR checks for example) for Asia and Australia Clients.
Actimize	ISG Trade Surveillance is a system that comprises of Trade Surveillance models and a case manager package that are used by Compliance and the Regulatory Control Group to comply with Industry regulations.

FC0	FCO Overnight regulatory confirmation system FCO is a Client trade confirmation system that delivers overnight official trade confirmations for Equity, Fixed Income, PWM and Prime Brokerage. It is a close relation to the FC3 system which delivers real time confirms for the same trades.
EPS (Expert Payment System)	Assessment system used to analyze cash payments leaving the Firm.
TAPS (RPU*) - Mainframe	RP is a real-time position keeper and P&L calculator within TAPS. It is used in the reconciliation of positions & P&L between TAPS and Risk. In addition it acts as a conduit of end of day marks from Risk to the Firms Back Office P&L Calculation System (PX).; Realtime position derived using Libra EOD + intra-day trading activities sourced from TAPS Trades File.
CMI	CMI is the cash management instruction system.
PIPE (Derivatives Client On-boarding)	PIPE Client On-Boarding and Maintenance Tool is a workflow tool designed to reduce firm risk and improve client service by creating a centralized workflow to efficiently manage the front to back client on-boarding process while enforcing proper business rules to ensure data quality and enforce regulatory requirements.
GIM2	PWM portfolio accounting system front end applications and database.

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

Deloitte Touche Tohmatsu
A.C.N. 74 490 121 060

Grosvenor Place
225 George Street
Sydney NSW 2000
PO Box N250 Grosvenor Place
Sydney NSW 1217 Australia

DX 10307SSE
Tel: +61 (0) 2 9322 7000
Fax: +61 (0) 2 9322 7001
www.deloitte.com.au

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")

Opinion

We have been engaged to report on MSWM's description in Section III of its internal controls over Private Wealth Management's ("PWM") custody services system and on the design and operation of controls related to the control objectives stated in the Section VI throughout the period from 1 July 2018 to 30 June 2019 (the description).

In our opinion, in all material respects, based on the criteria in Section II:

(a) The description fairly presents the PWM's custody services system as designed and implemented throughout the period from 1 July 2018 to 30 June 2019;

(b) The controls related to the control objectives stated in Section VI were suitably designed throughout the period from 1 July 2018 to 30 June 2019; and

(c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in Section VI were achieved, operated effectively throughout the period from 1 July 2018 to 30 June 2019.

Basis of Opinion

We conducted our engagement in accordance with Standard on Assurance Engagements ASAE 3402 *Assurance Reports on Controls at a Service Organisation*, and with reference to Guidance Statement GS 007 *Audit Implications of the Use of Service Organisations for Investment Management Services,* 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.

We have not evaluated the suitability of design or operating effectiveness of complementary user entity controls. The control objectives stated in the service organisation's description of its system can be achieved only if complementary user entity controls are suitably designed or operating effectively, along with the controls at the service organisation.

The following internal affiliates perform functions to support the custody services MSWM's provides to its PWM clients:

- MSIP – in the provision of custody services
- MSISG – in the provision of custody operations
- MSCL - in the provision of IT services

The inclusive method has been used in relation to the above, meaning MSWM's description of its PWM custody services system includes control objectives and related controls at the abovenamed internal affiliates. Our procedures extended to controls at the abovenamed internal affiliates to the extent they related to the custodial services.

Ausmaq is an external subservice organisation who perform functions on behalf of MSWM's custody services provided to PWM clients in relation to investor statement reporting. The carve-out method has been used in relation to Ausmaq. MSWM's description of its PWM custody services system excludes control objectives and related controls at Ausmaq, consequently our procedures did not extend to controls at Ausmaq.

Our opinion has been formed on the basis of the matters outlined in this report.

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

MSWM's Responsibilities

MSWM is responsible for: preparing the description and accompanying statement in Section II, 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 to achieve the stated control objectives.

Our Independence and Quality Control

We have complied with independence and other relevant ethical requirements relating to assurance engagements, and apply 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* in undertaking this assurance engagement.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on MSWM's PWM custody services system description and on the design and operation of controls related to the control objectives stated in that description**,** based on our procedures.

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 Section VI 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 (MSWM) and described in Section II.

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

Limitations of Controls at a Service Organisation

MSWM'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.

Description of Tests of Controls

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

Intended Users and Purpose

This report and the description of tests of controls in Section VI are intended only for customers who have used MSWM's PWM custody services and related information system, 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.

Liability limited by a scheme approved under Professional Standards Legislation.
Member of Deloitte Asia Pacific Limited and the Deloitte Network

Restriction of distribution and use

We disclaim any assumption of responsibility for any reliance on this report to any person other than the MSWM's clients and their auditors or for any purpose other than that for which it was prepared. This report is not intended to and should not be used or relied upon by anyone else and we accept no duty of care to any other person or entity.

Deloitte Touche Tohmatsu

Vincent Sita
Partner
Chartered Accountant
Sydney, 25 November 2019

Liability limited by a scheme approved under Professional Standards Legislation.
Member of Deloitte Asia Pacific Limited and the Deloitte Network

Section V:
Overview of the Work Performed

Deloitte.

Section V: Overview of the Work Performed

Introduction

This report on the description of the system is intended to provide 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 internal controls over Private Wealth Management's ("PWM") custody services system throughout the period 1 July 2018 to 30 June 2019.

Deloitte Touche Tohmatsu's engagement 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. Testing of MSWM's PWM controls was restricted to the control objectives and related control activities listed in Section VI and was not extended to controls that may be in effect at user organisations.

Deloitte Touche Tohmatsu's work was carried out at the premises of MSWM at Level 26, 2 Chifley Square, Sydney, NSW 2000 as well as across Asia, the US and UK. The scope of work was based on criteria (control objectives) agreed with management of MSWM prior to the commencement of work.

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 Touche Tohmatsu's procedures included tests of the following relevant elements of MSWM's control environment:

a) Overview of Operations and Applicability of Report
b) Business Structure
c) Control environment and risk management
d) Operations and Infrastructure Support functions
e) IT System

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 VI.

Obtaining Evidence Regarding the Description

Deloitte Touche Tohmatsu obtained and read the service organisation's description of its system in Section III, and evaluated whether those aspects of the description included in the scope of the engagement are fairly presented, including whether:

a) Control objectives stated in the service organisation's description of its system are reasonable in the circumstances;
b) Controls identified in that description were implemented;
c) Complementary user entity controls, if any, are adequately described; and
d) Services performed by a subservice organisation, if any, are adequately described, including whether the inclusive method or the carve-out method has been used in relation to them.

Obtaining Evidence Regarding Design of Controls

In determining which of the controls at the service organisation are necessary to achieve the control objectives stated in the service organisation's description of its system, Deloitte Touche Tohmatsu assessed whether those controls were suitably designed. This included:

a) Identifying the risks that threaten the achievement of the control objectives stated in the service organisation's description of its system; and
b) Evaluating the linkage of controls identified in the service organisation's description of its system with those risks. Some of the considerations Deloitte Touche Tohmatsu took into account included:
    - Appropriateness of the purpose of the control and its correlation to the risk/assertion
    - Competence and authority of the person(s) performing the control
    - Frequency and consistency with which the control is performed
    - Level of aggregation and predictability
    - Criteria for investigation (i.e. threshold) and process for follow-Up

Tests of operating effectiveness

Deloitte Touche Tohmatsu's tests of the controls were designed to cover a representative number of transactions throughout the period from 1 July 2018 to 30 June 2019. 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 tests of the control environment.

Testing the accuracy and completeness of information provided by MSWM is also part 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 utilised by MSWM.

While these procedures may not be specifically called out in the test procedures listed in Section VI, 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 performed a variety of tests relating to the controls listed in Section VI throughout the period from 1 July 2018 to 30 June 2019. The tests 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
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

Test	Description
	deviation 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.

a) The purpose of the procedure and the characteristics of the population from which the sample will be drawn when designing the sample;
b) Determine a sample size sufficient to reduce sampling risk to an appropriately low level;
c) Select items for the sample in such a way that each sampling unit in the population has a chance of selection;
d) If a designed procedure is not applicable to a selected item, perform the procedure on a replacement item; and
e) If unable to apply the designed procedures, or suitable alternative procedures, to a selected item, treat that item as a deviation.

The following guidelines are at a minimum followed in performing the test of controls:

Frequency of control activity	Minimum sample size
Annual	1
Quarterly	2
Monthly	2
Weekly	5
Daily	15
Many 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 identified (if any), were evaluated to conclude on whether the deviations are material individually or in combination.

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 Touche Tohmatsu 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 deviations in the way controls are applied by MSWM may occur. Deviations 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 deviations detected, the potential significance of the financial statement effect, as well as other qualitative aspects of the deviations such as the cause of the deviation.

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

If we find a single deviation in the 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.

Section VI:
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 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 customer 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 tested as part of this engagement.

Accepting Clients

A1 – New accounts are set up completely and accurately in accordance with client agreements and any applicable regulations.

Control Reference	Control Activity	Test Procedures	Results of Tests
A.1.A	A. The account opening forms are reviewed by the Branch Administration Management (BAM) Team after reviewing information provided and entered into NAO. From NAO the account flows through to Pipeline whereby AML (if required) reviews are performed. Once the data is entered into NAO, the BAM manager reviews for completeness and accuracy.	**Inspection** Inspected a sample of account opening forms and noted evidence of sign off from BAM and Legal regarding AML (Compliance) review where required.	No deviations noted
A.1.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 appropriate review and sign off by a supervisor. Additionally, confirmed that the account was properly set up in Qwest and corroborated by inspecting the details per Qwest to the account opening checklist including the date of the set-up, and the name of the account and other pertinent details	No deviations noted

A2 – Complete and authorised client agreements are established prior to initiating custody activity.

Control Reference	Control Activity	Test Procedures	Results of Tests
A.2	The General Terms form is signed off by the client prior to an account system set up.	**Inspection** Inspected a sample of General Terms form and verified sign off by the client prior to an account system set up.	No deviations noted

Authorising and processing of transactions

A3 – Investment and related cash and foreign exchange transactions are authorised and recorded completely, accurately and on a timely basis in accordance with client instructions.

Control Reference	Control Activity	Test Procedures	Results of Tests
A.3.A	Trade Processing Once trades have been executed by the Financial Adviser, a contract note is automatically generated by the FC3/FCO trade confirmation system and provided to the client.	**Observation** Observed the automatic generation of a contract note after trade details had been entered into the system. Tested to confirm the contract note was complete and accurate and provided to the correct client in a timely fashion.	No deviations noted
A.3.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 by BAM.	No deviations noted
A.3.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 checks on letters of authority and approval by BAM. Noted that there is segregation of duties.	No deviations noted
A.3.D	A 4 eye check for amounts that are < USD1M and 6 eye check (inputter and 2 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, completeness according to client instructions, appropriate four eyes/six eyes check and processing in a timely manner.	No deviations noted

A4 – 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.

Control Reference	Control Activity	Test Procedures	Results of Tests
A.4.A	SAFE automatically identifies daily settlement exceptions for the population of trades.	**Observation** Observed that SAFE system automatically identifies settlement exceptions. Tested the exception report for completeness and accuracy.	No deviations noted
A.4.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** Obtained and tested a sample of reconciliations and evidenced follow up on trade breaks by the settlements team.	No deviations noted

A5 – Corporate actions are identified, actioned, processed and recorded on a timely basis.

Control Reference	Control Activity	Test Procedures	Results of Tests
A.5.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. Tested the exception report for completeness and accuracy.	No deviations noted
A.5.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 deviations noted

Control Reference	Control Activity	Test Procedures	Results of Tests
A.5.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** Obtained and tested a sample of daily 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 deviations noted
A.5.D	High value/ risk issues are also escalated to MS internal functional management to ensure no client assets are in risk.	**Inspection** Obtained and tested a sample of daily reconciliations and evidenced that high value risk issues are escalated and reviewed by MS internal functional management.	No deviations noted

A6 – Cash receipts and payments are authorised, processed and recorded completely, accurately and on a timely basis.

Control Reference	Control Activity	Test Procedures	Results of Tests
A.6.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 daily cash receipts/payments requests and related status emails from maker to checker evidencing execution status and any follow-ups as necessary.	No deviations noted
A.6.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 deviations noted

A7 – 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 MSWM PWM clients.

Maintaining financial and other records

A8 – 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, loan services are not provided to MSWM PWM clients.

A9 – Collateral is completely and accurately invested in accordance with the lender's agreement.

Not applicable, collateral is not obtained from MSWM PWM clients.

A10 – Accounts are administered in accordance with client agreements and any applicable regulations.

Control Reference	Control Activity	Test Procedures	Results of Tests
A.10.A	The firm's risk systems, including Actimize, Compliance Monitoring Inventory (CMI), and Client Suitability Engine (CSE), 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.	**Inspection** Inspected a sample of automated e-mails from the system to the Financial adviser, containing breach specifications, to confirm timely follow up e-mail to the Risk team requiring further action.	No deviations noted
A.10.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 IWM Short Term Trading Reports, Black Out Trade International Reports and Equity Solicitation Violation Report to verify whether reviews were performed to ensure adherence to appropriate regulatory requirements.	No deviations noted

Control Reference	Control Activity	Test Procedures	Results of Tests
A.10.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 deviations noted

A11 – Changes to non-monetary static data (for example, address changes and changes in allocation instructions) are authorised and correctly recorded on a timely basis.

Control Reference	Control Activity	Test Procedures	Results of Tests
A.11.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 deviations noted
A.11.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 deviations noted

A12 – 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 - MS does not provide a reclaim service for MSWM PWM clients.

A13 – Asset positions for securities held by third parties such as sub custodians and depositories are accurately recorded and regularly reconciled.

Control Reference	Control Activity	Test Procedures	Results of Tests
A.13.A	A reconciliation between banks 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. Tested the completeness and accuracy of the reconciliation and evidenced that discrepancies are followed up by the global reconciliation team, investigated and assigned for resolution.	No deviations noted
A.13.B	In the event of a Stock position 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 flag breaks identified, during the system reconciliation. Tested the completeness and accuracy of the reconciliation. Evidenced follow up from the Settlements team to business units for investigation and resolution of breaks.	No deviations noted

Safeguarding assets

A14 – Assets held (including investments held with depositories, cash and physically held assets) are safeguarded from loss, misappropriation and unauthorised use.
A15 – Assets held are appropriately registered and client money is segregated.

Control Reference	Control Activity	Test Procedures	Results of Tests
A.14.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 a sample of Custodian Agreements and Asset Segregation letters to evidence segregation] of client money and responsibilities. Inspected a sample of Trust Acknowledgement Letters to evidence the rules set out in the CASS were followed.	No deviations noted
A.14.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 deviations noted
A.14.C	Matters related to assets held by third parties are discussed during the monthly Assets Governance Committee meeting.	**Inspection** Inspection of evidence of Client Assets Governance Committee meetings throughout the audit period to evidence that client money and assets is discussed in the meeting.	No deviations noted
A.14.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** Inspected a sample of internal reconciliations between internal books and Agents records and evidenced that discrepancies were investigated. Refer to A.13.A for external reconciliation test procedures.	No deviations noted

Monitoring compliance

A16 – Transaction errors are rectified promptly.

Control Reference	Control Activity	Test Procedures	Results of Tests
A.16.A	The financial adviser must inform BAM as soon as they become aware of the necessity of correcting a trade on the back of a trade error made and rebooking. The financial adviser has to complete and sign off on an error & rebooking form, detailing the impacted client, advisor code and reason for the errors made. The error & rebooking form is checked and signed off by Branch risk team, who instructs PWM BAM to approve and notifies Trade Support team to rebook trades as soon as possible.	**Inspection** Inspected a sample of error forms and evidenced sign off/approval by BAM and notifications sent to trade support for rectification as soon as possible.	No deviations noted
A.16.B	A monitoring report capturing all cancel and corrects is reviewed by BAM, who reconcile the report with the cancel & correct forms on file, to ensure the cancel & corrects have been duly recorded. This report is signed off by BAM to evidence review and follow up.	**Inspection** Inspected a sample of cancel and correction forms, checked these against the daily reconciliation report, and evidenced approval by BAM and instructions triggered via workflow system to operations for rectification.	No deviations noted
A.16.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 deviations noted

Monitoring Subservice Organisations

A17 – 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.

Control Reference	Control Activity	Test Procedures	Results of Tests
A.17.A	MS Global Network Management team assess custodians and agent banks suitability on an ad-hoc basis, based on a list of considerations	**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. For the Annual Due Diligence of providers, refer to A14.B.	No deviations noted
A.17.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 deviations noted
A.17.C	Incidents with providers are logged into the Global system and until resolution.	**Inspection** Inspected a sample of incidents and obtained evidence of recording and monitoring in the Global Incident Network.	No deviations noted

Reporting

A18 – Client reporting in respect of client asset holdings is complete and accurate and provided within required timescales.

Control Reference	Control Activity	Test Procedures	Results of Tests
A.18.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 Intellimatch and Safe 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 completely and accurately in the Exception Monitoring tool, for investigation and resolution.	No deviations noted
A.18.B	Monthly Asset Under Management (AUM) figures are verified and sample checked against the month end official statement generated.	**Inspection** Inspected a sample of monthly asset under management reports and evidenced checks performed against the official statement, with discrepancies investigated.	No deviations noted
A.18.C	Monthly statement delivery reconciliation is performed to ensure clients receive their online and physical statements by KRI (Key Risk Indicator) date of Business Day 10. Statement exceptions are identified and resolved daily until all client statements are sent.	**Inspection** Inspected a sample of monthly statement delivery reconciliations and evidenced that over 99% of physical and electronic statements were sent to clients during the following month. We confirmed that exceptions are identified and resolved daily until all client statements are sent.	No deviations noted

A19 – Asset positions and details of securities lent (including collateral) are reported to interested parties accurately and within the required time scale.

Not applicable, securities lending is currently not offered to MSWM PWM clients.

Information Technology

G1 - Physical Access to computer networks, equipment, storage media and program documentation is restricted to authorised individuals

Control Reference	Control Activity	Test Procedures	Results of Tests
G.1.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 deviations noted
		Webstreme (Ausmaq Third party software) **Inspection** Confirmed MSWM monitor Ausmaq and inspected the Ausmaq ASAE 3402 report to validate the effectiveness of internal controls related to physical access policies, physical access, storage of media and datacentre security devices.	No deviations noted

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

Control Reference	Control Activity	Test Procedures	Results of Tests
G.2.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 deviations noted
		Webstreme (Ausmaq Third party software) **Inspection** Confirmed MSWM monitor Ausmaq and inspected the Ausmaq ASAE 3402 report to validate the effectiveness of internal controls related to Password access policy settings and system configuration.	No deviations noted

Control Reference	Control Activity	Test Procedures	Results of Tests
G.2.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 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 deviations noted
G.2.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 deviations noted

Control Reference	Control Activity	Test Procedures	Results of Tests
G.2.D	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. 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.	**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 deviations noted

Webstreme (Ausmaq Third party software) **Inspection** Confirmed MSWM monitor Ausmaq and inspected the Ausmaq ASAE 3402 report to validate 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 role 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. **Webstreme (Ausmaq Third party software)** **Inspection** Confirmed MSWM monitor Ausmaq and inspected the Ausmaq ASAE 3402 report to validate the effectiveness of internal controls related to employee restricted access to privileged functions. **Observation**	No deviations noted

Control Reference	Control Activity	Test Procedures	Results of Tests
		Through observation conducted with the platform owner, privileged access is granted to Webstreme by authorised system administrators. **Webstreme (Ausmaq Third party software)** **Inspection** Confirmed MSWM monitor Ausmaq and inspected the Ausmaq ASAE 3402 report to validate the effectiveness of internal controls related to application users 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

Control Reference	Control Activity	Test Procedures	Results of Tests
G.3.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 deviations noted
		Webstreme (Ausmaq Third party software) **Inspection** Confirmed MSWM monitor Ausmaq and inspected the Ausmaq ASAE 3402 report to validate 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	No deviations noted

		• 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.	
G.3.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. 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.	**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 deviations noted
		Webstreme (Ausmaq Third party software) **Inspection** Confirmed MSWM monitor Ausmaq and inspected the Ausmaq ASAE 3402 report to validate 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	No deviations noted

		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.	
G.3.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 deviations noted
		Webstreme (Ausmaq Third party software) **Inspection** Confirmed MSWM monitor Ausmaq and inspected the Ausmaq ASAE 3402 report to validate 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.	No deviations noted

		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.	
G.3.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 deviations noted
		Webstreme (Ausmaq Third party software) **Inspection** Confirmed MSWM monitor Ausmaq and inspected the Ausmaq ASAE 3402 report to validate 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 deviations noted
G.3.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.	No deviations noted

		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 Section G.3A, G.3B, G.3C, G.3D above	
		Webstreme (Ausmaq Third party software) **Inspection** Confirmed MSWM monitor Ausmaq and inspected the Ausmaq ASAE 3402 report to validate 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 deviations noted

G4 - IT Processing is authorised and scheduled appropriately and exceptions are identified and resolved in a timely manner

Control Reference	Control Activity	Test Procedures	Results of Tests
G.4.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	No deviations noted

		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.	
		Webstreme (Ausmaq Third party software) **Inspection** Confirmed MSWM monitor Ausmaq and inspected the Ausmaq ASAE 3402 report to validate 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 deviations noted

G.4.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 successfully rerun or the incidents were escalated and tracked to resolution.	No deviations noted
		Webstreme (Ausmaq Third party software) **Inspection** Confirmed MSWM monitor Ausmaq and inspected the Ausmaq ASAE 3402 report to validate the effectiveness of internal controls related to the logging and resolution of a	No deviations noted

		sample of jobs to determine whether it was resolved in a timely manner.	

G5 - Appropriate measures, including firewalls and anti-virus software, are implemented to counter the threat from malicious electronic attack

Control Reference	Control Activity	Test Procedures	Results of Tests
G.5.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 deviations noted
		Webstreme (Ausmaq Third party software) **Inspection** Confirmed MSWM monitor Ausmaq and inspected the Ausmaq ASAE 3402 report to validate 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	No deviations noted

	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.	

G6 - The physical IT equipment is maintained in a controlled environment

Control Reference	Control Activity	Test Procedures	Results of Tests
G.6.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 deviations noted
		Webstreme (Ausmaq Third party software) **Inspection** Confirmed MSWM monitor Ausmaq and inspected the Ausmaq ASAE 3402 report to validate 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 deviations noted

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.

Control Reference	Control Activity	Test Procedures	Results of Tests
G.7.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 deviations noted

Control Reference	Control Activity	Test Procedures	Results of Tests
G.7.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 deviations noted

Control Reference	Control Activity	Test Procedures	Results of Tests
G.7.C	Application changes to the Morgan Stanley's distributed environment (applications and jobs) are documented, tested, and approved prior to implementation into production. The distributed environment utilizes automated tools (i.e., VMS and Autosys) together with the EDM system to migrate changes into production. In order to migrate a change into production, the turnover tools require an approved Technology Change Management (TCM) ticket. An approved TCM ticket requires appropriate signoff from key stakeholders (e.g., technology owner, business unit, and operations) depending on the severity of the change. EDM correlates the turnover request with an approved TCM ticket in terms of the application name, production location of files to be moved, and the time and date of turnover. If the change request does not have an approved TCM ticket or the required turnover details do not correlate, EDM will prevent the change from being moved into production.	**Observation** Through observation with Morgan Stanley Change Management personnel, ascertained that the distributed environment utilized automated change tools to migrate changes into production and a change required an approved TCM ticket that appropriately correlates with the application name, production location of files to be moved, and the time and date of turnover. **Observation** Through observation of turnover tools configurations, ascertained that the tools prevent a change from being turned over into production when it was not associated with an approved TCM. **Inspection** For a selection of changes in the distributed environment, ascertained through inspection of the change documentation that changes were documented, tested, and approved prior to implementation into production.	No deviations noted

Control Reference	Control Activity	Test Procedures	Results of Tests
G.7.D	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 conversion of information technology, in order to minimize disruptions to operations.	**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	**Deviation noted** EDM validation, which is intended to prevent post approval modifications made to SYTS, DB2TS and GPTS distributed database resources prior to release, was not configured as intended. As a result, changes could be made to database resources after the All Approved Date and prior to the execution of the turnover (release into production). A mitigating control has been identified and tested, refer to G.7.E. Please refer to Appendix B for further details and Management's Response.

Webstreme (Ausmaq Third party software) **Inspection** Confirmed MSWM monitor Ausmaq and inspected the Ausmaq ASAE 3402 report to validate 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 deviations noted
Webstreme (Ausmaq Third party software) **Inspection** Confirmed MSWM monitor Ausmaq and inspected the Ausmaq ASAE 3402 report to validate 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.	

Control Reference	Control Activity	Test Procedures	Results of Tests
G.7.E	For distributed database resources, Quality Assurance & Production Management (QAPM) team identifies changes that were made to database resources between the "All Approved" date and "Turnover" date. For each change, the QAPM team performs a review to assess the nature and type of the change with the IT System Owners to determine if the change was authorized. All changes from the review are researched and tracked to resolution.	**Inspection** For the full population of distributed databases changes, ascertained through inspection of documentation that QAPM team identified changes that were made to database resources between "All Approved" date and "Turnover" date and the root cause and impact analysis for those changes post verification to confirm those were appropriate and authorized. Confirmed that all changes were researched and tracked to resolution.	No deviations noted
G.7.F	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") provides monitoring reports to individual CIOs and their delegated representatives to provide the root cause of the use of emergency changes.	**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 deviations noted

Control Reference	Control Activity	Test Procedures	Results of Tests
G.7.G	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.	**ISG Mainframe** **Observation** Observed that in the mainframe environment, emergency changes follow the same process as non-emergency changes.	No deviations noted

G8 - Data Migration or modification is authorised, tested and, once performed, reconciled back to the source data

Control Reference	Control Activity	Test Procedures	Results of Tests
G.8.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** Confirmed MSWM monitor Ausmaq and inspected the Ausmaq ASAE 3402 report to validate 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 deviations noted

G9 - Data and systems are backed up regularly offsite and regularly tested for recoverability on a periodic basis

Control Reference	Control Activity	Test Procedures	Results of Tests
G.9.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 deviations noted

Control Reference	Control Activity	Test Procedures	Results of Tests
		Webstreme (Ausmaq Third party software) **Inspection** Confirmed MSWM monitor Ausmaq and inspected the Ausmaq ASAE 3402 report to validate 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 deviations noted

G10 - IT Hardware and software issues are monitored and resolved in a timely manner

Control Reference	Control Activity	Test Procedures	Results of Tests
G.10.A	The problem management process ensures that the production environment, including	Refer to G4	Refer to G4

Control Reference	Control Activity	Test Procedures	Results of Tests
	hardware, network, backups, and database problems are captured, tracked and addressed.	**Webstreme (Ausmaq Third party software)** **Inspection** Confirmed MSWM monitor Ausmaq and inspected the Ausmaq ASAE 3402 report to validate 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 deviations noted

G11 - Business and information systems recovery plans are documented, approved, tested and maintained

Control Reference	Control Activity	Test Procedures	Results of Tests
G.11.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 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.	**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 deviations noted
		Webstreme (Ausmaq Third party software) **Inspection** Confirmed MSWM monitor Ausmaq and inspected the Ausmaq ASAE 3402 report to validate 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.	No 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 clients.

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

Control Reference	Control Activity	Test Procedures	Results of Tests
G.13.A	Contracts are in place for 3rd party service providers. SLA's are monitored and reported to management quarterly. Controls operating at the third party IT application provider are monitored on a periodic basis.	**Inspection** Inspected the executed Webstreme Ausmaq contract in place. Inspected quarterly minutes of meetings with Ausmaq to evidence monitoring of Ausmaq's services including review of SLA performance and follow up outstanding action items.	No deviations noted

Section VII: Other Information Provided by the Service Organisation that does not form part of Deloitte Touche Tohmatsu's Opinion

Section VII: Other Information provided by the Service Organisation that does not form part of Deloitte Touche Tohmatsu's Opinion

The information included in this Section of the report is presented by Morgan Stanley Wealth Management Australia Pty Ltd ("MSWM") to provide additional information to customers and is not part of the MSWM's description of the system nor the Service Auditor's Assurance Report.

The information included in this Section has not been subjected to the test procedures performed by the service auditor as detailed in Section VI, accordingly, Deloitte Touche Tohmatsu does not express an opinion on it.

Management's response to deviations noted:

Control Reference	Control Activity	Deviation Noted	Management Response
G.7.D	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 conversion of information technology, in order to minimize disruptions to operations.	EDM validation, which is intended to prevent post approval modifications made to SYTS, DB2TS and GPTS distributed database resources prior to release, was not configured as intended. As a result, changes could be made to database resources after the All Approved Date and prior to the execution of the turnover (release into production). A mitigating control was identified and tested, refer to G.7.E.	Management has confirmed that the configuration has been remediated. An analysis was performed and based on the results of the analysis, management confirmed the prior configuration did not impact any of the applications in scope for this report.