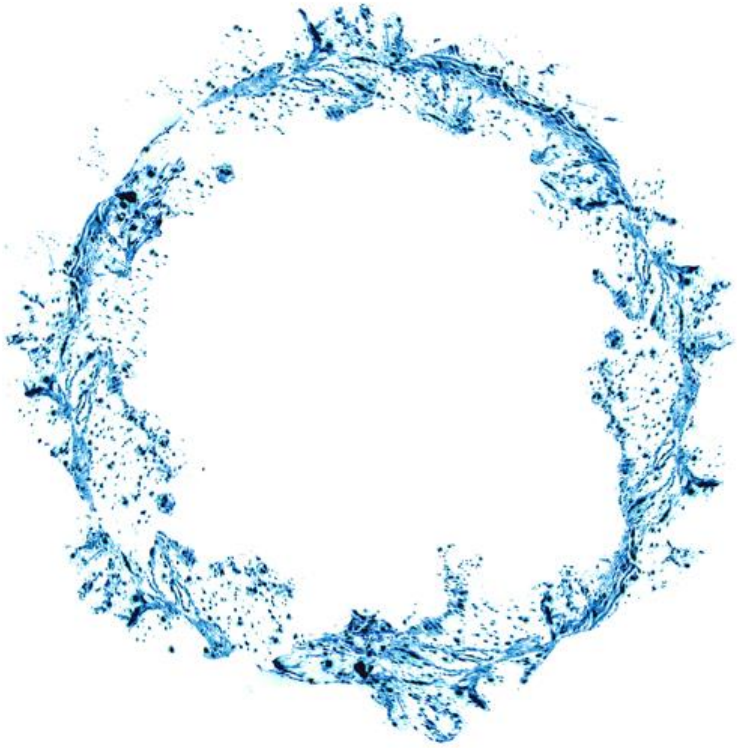
Morgan Stanley



Private Wealth Management Custody Services of Morgan Stanley Wealth Management Australia Pty Ltd

ASAE 3402 Type 2 Service Organisation Controls Report

For the period 1 July 2022 to 30 June 2023

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, and that transactions are valid. In addition, ensuring 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 2022 to 30 June 2023, 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 Organisation* ("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 2022 to 30 June 2023 unless otherwise indicated.

This report includes controls operated by internal affiliates of MSWM who perform functions to support the custody services MSWM provides to its PWM clients however, this report does not include other services provided by MSWM, that are not outlined in the description of systems and controls below.

In addition to the exclusion noted above, this report does not include controls at external sub-service organisations of MSWM and complementary user entity controls, which are the controls assumed to be implemented by clients for stated control objectives to be met. 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, which are listed in Section VI.

The Independent Service Auditor's Assurance Report provided by Deloitte on the description of controls, their design and operating effectiveness over custody services, was an unmodified opinion. That opinion is included in Section IV, Independent Assurance Report, within this Controls Report.

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.	No deviations noted	Control objective met.
A.2 Complete and authorised client agreements are established prior to initiating custody activity.	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.	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.	No deviations noted	Control objective met.
A.5 Corporate actions are identified, actioned, processed and recorded on a timely basis.	No deviations noted	Control objective met.
A.6 Cash receipts and payments are authorised, processed and recorded completely, accurately and on a timely basis	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 – MSWM does not provide its PWM clients securities lending services.	
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 – MSWM does not provide its PWM clients loan services.	
A.9 Collateral is completely and accurately invested in accordance with the lender's agreement.	N/A – MSWM does not provide its PWM clients securities lending services.	
A.10 Accounts are administered in accordance with client agreements and any applicable regulations.	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.	No deviations noted	Control objective met.
A.12 Investment income and related tax reclaims are collected and recorded accurately and on a timely basis.	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.	No deviations noted	Control objective met.
A.14 Assets held (including investments held with depositories, cash and physically held assets) are safeguarded from loss, misappropriation and unauthorised use.	No deviations noted	Control objective met.

Control Objective	Results	Conclusion (in all material respects)
A.15 Assets held are appropriately registered and client money is segregated.	No deviations noted	Control objective met.
A.16 Transaction errors are rectified promptly.	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.	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.	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 – MSWM does not provide its PWM clients securities lending services.	
Information Technology		
G.1 Physical access to computer networks, equipment, storage media and program documentation is restricted to authorised individuals.	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.	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.	Deviations noted in 2 controls. Refer to Section VI for details and Section VII for management response	Control objective met.
G.4 IT processing is authorised and scheduled appropriately and deviations are identified and resolved in a timely manner.	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.	No deviations noted	Control objective met.
G.6 The physical IT equipment is maintained in a controlled environment.	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.	No deviations noted	Control objective met.
G.8 Data migration or modification is authorised, tested and, once performed, reconciled back to the source data.	No instances of the control were operated during the period as there were no relevant data migrations	Not applicable.
G.9 Data and systems are backed up regularly offsite and regularly tested for recoverability on a periodic basis.	No deviations noted	Control objective met.

Control Objective	Results	Conclusion (in all material respects)
G.10 IT hardware and software issues are monitored and resolved in a timely manner.	No deviations noted	Control objective met.
G.11 Business and information systems recovery plans are documented, approved, tested and maintained.	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 – MSWM does not provide IT services to its PWM clients.	
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.	N/A – MSWM has not engaged IT sub-service organisations.	

Section II:
Statement by the Service Organisation

Morgan Stanley

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

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

(a) The accompanying description in Section III fairly represents the PWM custody services provided to clients throughout the period 1 July 2022 to 30 June 2023. To ensure continuity, the criteria used in making this statement had the accompanying description:

i. How the system was designed and implemented, including:

- The types of services provided, including, classes of transactions processed (if applicable).
- The procedures, within both information technology and manual systems, by which those transactions were initiated, recorded, processed, corrected (if applicable) and transferred to the clients report.
- The related accounting records, supporting information and specific accounts that were used to initiate, record, process, and report transactions. This includes the correction of incorrect information and how information was transferred to the reports prepared for clients.
- How the system dealt with significant events and conditions, other than transactions.
- The process used to prepare reports for clients.
- Relevant control objectives and controls designed to achieve those objectives.
- Controls that we assumed, in the design of the system, would be implemented by clients, 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 including: risk assessment process, information system (including the related business processes), communication, control activities and monitoring controls that were relevant to processing and reporting clients' transactions.

ii. Includes relevant details of changes to MSWM's system during the period 1 July 2022 to 30 June 2023.

iii. Does not omit or distort information relevant to the scope of the system being described, while acknowledging that the description is prepared to meet the common needs of a broad range of clients and their auditors. Therefore, it may not include every aspect of the system that each individual client may consider important in its own particular environment.

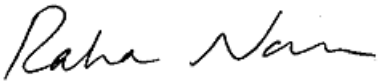
(b) The controls related to the control objectives stated in the accompanying description were effectively designed and operated effectively throughout the period 1 July 2022 to 30 June 2023. The criteria used in making this statement were that:

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

ii. The identified controls, if operated as described, would 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 2022 to 30 June 2023.

Signed on behalf of Management of MSWM.



Raha Nasseri
Chief Operating Officer
Morgan Stanley Wealth Management

19 December 2023

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, mutual funds, 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"). 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 agent 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

The 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 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 with internal 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 mentioned areas above, the operational and technology controls are the responsibility of MSWM however many are operated by MSWM internal affiliates. Controls at internal affiliates MSIP and MSCL 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 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 monitored by Morgan

Stanley's Global Network Management department. The report does not extend to the controls of sub-custodians. See further details in Section 5 below.

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 source of wealth. This includes the client's short and long-term goals and concerns, the structure of any current holdings, and the client's exposure to and tolerance for risk.

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

Morgan Stanley's PWM platform clients receive real-time access to their portfolios via Matrix, the MSWM client web portal, 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 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 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:

a) The risks that threatened achievement of the control objectives stated in the description were identified;

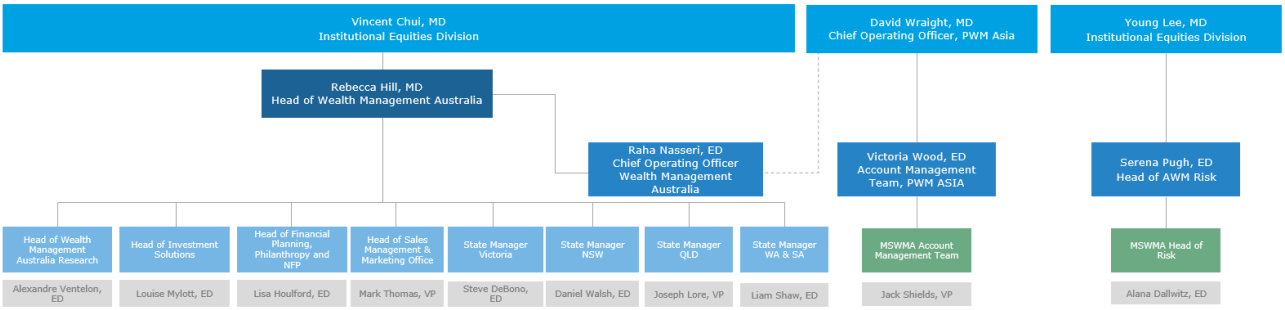
b) The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved; and
c) The description of the controls and control environment does not omit relevant information.

1.4 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 2023 is shown below:



Functional Groups

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

Group	Function
Account management Team (AMT)	New account onboarding and maintenance
Risk Management	Risk monitoring Error Handling Product and Investment Suitability 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
Client Onboarding and Regulatory Service (CORS)	AML/KYC documentation review and sign off

1.5 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 mandatory training and education sessions 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, and gifts and entertainment.

1.6 Assignment of Authority and Responsibility

The control environment is 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:

a) 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); and
b) Compliance, Legal and Audit are separate functions and provides compliance and monitoring oversight across the business.

1.7 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. Internal audit reports, which carry a rating and outline the degree to which unacceptable risk exposures were identified, are presented to senior management. The internal 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 internal audit findings and to indicate target dates as to when appropriate corrective action will be completed.

1.8 Risk Management

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

a) Credit Risk: The most significant credit risk is that margin loans granted to clients are not repaid (including risks associated with managing the collateral lodged by clients);
b) 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);
c) 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; and
d) 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:

a) Insurance Policies: MSMW maintains adequate levels of insurance and is reviewed on a yearly basis.
b) 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.
c) 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.

1.9 Information and Communication

Information and communication are 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 via training and written communication (such as email), significant business events and other major announcements by written and verbal communication. 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. Morgan Stanley has various global policies in place governing this.

1.10 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 to regular reviews and are endorsed by the relevant Management or Risk Committee.

MSWM's compliance manual is subject to an annual review.

These included:

a) 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).
b) 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).
c) Breach Reporting: MSWM Compliance Department maintains a breach register. This is monitored and reported to the Board.

1.11 Complementary 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:

a) 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 Refer to A2, A3, A6 & A11.
b) 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. Refer to A2, A3, A6 & A11.
c) 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. Refer to A2, A3, A6 & A11.
d) User entities should provide MSWM with timely written notification regarding changes to those individuals authorised to instruct on behalf of client activities. Refer to A2, A3 & A6.
e) User entities should periodically review standing instructions provided to MSWM Refer to A2, A3 & A6.
f) User entities should establish, monitor and maintain effective controls over physical and logical access to their computer systems via PCs at client locations. Refer to A2, A3 & A6.
g) 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. Refer to A16.
h) User entities should provide timely tax information to MSWM to ensure the efficient completion of year-end reporting Refer to A12 & A18.

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.

2 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:

a) Information Technology
b) Operations
c) Legal and compliance

d) Risk management
e) Tax
f) Financial and regulatory controls, and
g) Treasury

As part of the delegated operations services provided by MSIP to MSWM, 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 Institutional Securities Group (MSISG) Operations as outlined below:

a) MSISG handles for MSWM's PWM clients 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.
b) 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.

3 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.

The Morgan Stanley organisation engages with a large number of sub-custodians and agent banks in the delivery of its PWM services. The PWM Global Network Management team is tasked with ongoing monitoring of these sub-custodians and agent banks through a due diligence questionnaire. The team prepare an annual due diligence report which outlines the risk ratings, assessment of sub-custodian organisation and agent banks covering safe custody of client assets, operational and financial risk, issues identified and follow-up actions. The report and a checklist are subsequently reviewed and signed off by a member of the Due Diligence Review team, Country Officer and Country Manager.

This report does not include controls at any 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.

4 IT Systems

4.1 Network and Infrastructure

MSWM PWM utilises both mainframe and distributed technology. The key system platforms are standardised on z/OS, Linux and Windows operating systems. Morgan Stanley owns and operates the Data Centres located in Somerset and Piscataway, New Jersey USA; iAdvantage and GlobalGateway, Hong Kong and Heathrow and Croydon in the UK

4.2 Information Technology Organisation

Morgan Stanley IT is divided into the business units with a Hong Kong based IT Managing Director heading up PWM IT from a regional perspective. 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, organised by function, to the functional area that is leading and managing that project.

Morgan Stanley's Enterprise Technology & Services ("ETS") is responsible for each business line's server management and deployment needs, providing adherence to Morgan Stanley IT standards. While the responsibility is centralised, the specialised support groups are resident in each location. Specialised 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 Cyber Data Risk & Resilience.

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 at all times. Refer below to 4.4 for further details.

4.3 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.

As part of business continuity planning, Business Units must identify and assess the potential impact of threats that may significantly disrupt their business or the business operations of the Firm. Business continuity plans document recovery strategies (e.g., transference or work area recovery) that identify and detail the options available to recover critical business processes during an incident. The plans also identify roles and responsibilities and communication procedures when plans are invoked for an incident.

Business Units are responsible for periodic testing and documentation of test results in accordance with the requirements set out in the Global Business Continuity Testing Procedure. Business continuity testing is the process by which Business Units verify the viability of their plans by performing their critical business processes using the recovery strategies documented in the plans. Business continuity testing and documentation of test results provide a reasonable expectation that, during a business continuity incident, the Business Unit will be able to recover and perform its critical business processes and limit the impact of the incident to the Firm, its clients, and financial markets.

Morgan Stanley's primary data centers are built to be redundant, resilient and fault tolerant. Synchronous replication is used to provide high availability of critical applications. Disaster recovery plans supporting business continuity are in place for critical facilities and resources across the firm. These plans define recovery times that vary according to the criticality of businesses and functions.

4.4 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 client 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 (PWM CMS)	IWM Client Management is the client data repository for the PWM Asia, Australia business that also provides access to business users. Client Management system sources data from firms systems and PWM systems and processes it to provide client information for PWM systems to consume client data. The Client Management Application allows users to access detailed client and account information. Using the application, business users can view client contact details, eligibility, suitability, GDS documentation, KYC/AML/MIFID status.
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 clients. Data from the Intellimatch system is downloaded to a number of risk tracking and management reporting functions. A variety of operations group use Intellimatch for their daily reconciliation needs. Some of the groups include, SSBO (Shared Service & Banking Operations), ORRC (Operations Risk & Regulatory Control), ISG Product Operations (ISGPO), Wealth Management Operations (WM Ops) amongst others. Intellimatch uses a centralized Informatica plant to source in/out data for reconciliation. Data is loaded into MSSQL database server for performing the reconciliation. All Intellimatch components are run from windows environment and the supporting data sourcing system (Informatica) is run on Linux.
QWEST	QWEST (Query Workflow Exceptions Services Technology) is an Enterprise-wide application that consolidates information from many underlying data sources into one portal.

Application	Description
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	Scorpio provides systematic solutions and operations controlled workflow to process global corporate actions and dividends including event capture, entitled position capture, election capture and authorization, entitlement calculation and payment distribution functions.
STP Workstation	PWM STP Workstation is a PWM Proprietary order entry and order management system. It supports Equities, Options, OTC's and Mutual Funds It performs order capture, pre-trade checks, execution and client side booking support.
PWM NAO Client Account Management and Onboarding system (CAMO)*	PWM New Account Opening application used to onboard a new PWM client. From FY24 this will be replace by CAMO which has been run in parallel with NAO since 19 June 2023.
PWM AI*	PWM AI is a PWM Proprietary order entry and order management system. It supports Alternative Investments. It performs order capture, pre-trade checks, execution and client side booking support.
NISA*	New Issues Subscription & Allocation (NISA) Fixed Income application.
T2	T2 is a legacy trade capture for Equity OTC derivative trades and positions. The system is used by Equity Derivatives Sales and Trading Users and their Support Groups (i.e. Operations, Finance, etc.). T2 OTC Functions are being replaced by TX/LCM System.
LiveWire	LiveWire GUI enables maintenance & tracking of deals, rates and clients in Wire, track charges in Global Billing System and create overrides.
ASRV	Asset Services Applications (ASRV) is used to support corporate action notification and response (elections and proxy voting services).
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: Control reporting - reports/alerts to facilitate users to perform control/monitoring functions Data integration - data exchange between MS and external system in a variety of data formats Data integrity check - detect data integrity issue before further user or downstream processing.
Client Suitability Engine (CSE)	This comprises of assets for Client Suitability and Eligibility suite of applications - which comprises Web application (UI) and middle tier services (and internally used within Morgan Stanley ONLY - not exposed outside Morgan Stanley network) - which are used to: Source Client, Product, Positions, Transactions etc from upstream systems To assess / evaluate Client's Suitability and Eligibility - for pre and post trade checks - based on defined Risk evaluation / validation rules (Product Risk Rating based checks for example) And also to support, Product Due Diligence process, Risk metric setup process, Post trade reconciliation / Mismatch approval and surveillance process For - PWM Asia and Australia Business - Clients (represented via Sales / CSR/IR), Risk Team, Product Due Diligence Team etc.
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.

Application	Description
EPS (Expert Payment System)*	Expert Payment System (EPS) is a Payment Validation Application used by Treasury to centrally manage wire payments (free cash) across several Firm Settlements Systems and to systemically assess them for a variety of exceptions that defend against regulatory violations, improper formatting, fraud, and other operational risks. EPS is a global system, used in New York, London, Tokyo, and Hong Kong. This application is used for multiple business lines.
Compliance Management Dashboard	Compliance Management Dashboard is primarily focused on 4 aspects: 1) Compliance Monitoring Inventory (CMI): This is a central Inventory for Compliance Monitoring Business Activities and hosts monitoring activities by operations. 2) Monitoring Checks: This is a central repository to maintain list of all monitoring checks - adhoc testing that compliance performs. 3) MSRT: MSRT utility is responsible for generating quality check alerts for various business units across the firms based on global compliance policy sampling requirements. 4) CMD: Provide metrics data to populate dashboards for compliance management.
Client RefData Mgmt (CRD/PIPE)	This covers the applications, database and service platform supporting client on-boarding and client data and document refresh. The business processes include, client onboarding creation and approval, and periodic maintenance of client data and documents. These business processes exist to support AML / KYC regulatory requirements.
Libra and Operational GUIs	Libra is the TAPS Position & Balance subledger. Libra contains the P&B data and the journal audit trail forming this data. Libra also contains the JEMS (Renovated Manual Journal System).
MSPA-IVWM Reporting	MSPA Cost Accounting Engine for all ISG businesses. The Backend GRN performing all the key accounting functionality is the mspa3 grn (EON 13572) This is the reporting database part of the functionality; and the user interface part IWM Asia/AU/EMEA business. A separate GRN is being opened as this part of the application handles PII
PWMSecure	PWM-wide entitlement system which allows granting of application and data permissions to internal users.
PARI*	PARI is the strategic post-settlement operational reconciliation tool for OTC derivative cash settling products, used primarily for identification, tracking and reporting of settlement fails. Pari matches and groups journals posted to client accounts and uses various other data (contractual cashflows, linkage to payment instructions and open SAFE missions) to identify and help investigate and resolve settlement fails.

* These applications do not include automated controls or reports which are relied upon to achieve the control objectives in scope of this report and therefore have not been included in the scope of testing for the IT objectives and controls.

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

Quay Quarter Tower
50 Bridge Street
Sydney NSW 2000
PO Box N250
Sydney NSW 1217 Australia

DX 10307SSE
Tel: +61 (0) 2 9322 7000
Fax: +61 (0) 2 9322 7001

Deloitte.

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 2022 to 30 June 2023 (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 2022 to 30 June 2023;

(b) The controls related to the control objectives stated in Section VI were suitably designed throughout the period from 1 July 2022 to 30 June 2023; and

(c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in Section VI were achieved, operated effectively throughout the period from 1 July 2022 to 30 June 2023.

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:

- Morgan Stanley & Co International plc: In the provision of custody services
- Morgan Stanley & Co LLC: In the provision of IT services.

The inclusive method has been used in relation to the above internal affiliates, 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.

The subservice organisations referred to in Section III part 5 "Key Third Party / External Subservice Organisations" perform functions for MSWM's PWM custody services . The carve-out method has been used in relation to them. MSWM's description of its PWM custody services system excludes control objectives and related controls at these subservice organisations, consequently our procedures did not extend to controls at these subservice organisations.

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 Management

We have complied with independence and other relevant ethical requirements relating to assurance engagements, and apply Auditing Standard ASQM 1 *Quality Management for Firms that Perform Audits and Reviews of Financial Reports and Other Financial Information or Other Assurance or 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 clients and their auditors and may not, therefore, include every aspect of the system that each individual client may consider important in its own particular environment. Also, because of their nature, controls at a service organisation may not prevent or detect all errors or omissions in processing or reporting transactions. Also, the projection of any evaluation of effectiveness to future periods is subject to the risk that controls at a service organisation may become inadequate or fail.

Description of Tests of Controls

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

Other Information

Management is responsible for the other information. The other information comprises the information included in Section I Executive summary and Section VI Other information provided by the Service Organisation that does not form part of our Opinion for the year ended 30 June 2023 but does not include the Statement in Section II, Description in Section III and the control objectives and controls stated in Section VI and our service auditor's report thereon.

Our opinion on the description in Section III and on the design and operation of controls related to the control objectives stated in Section VI does not cover the other information and we do not express any form of assurance conclusion thereon.

In connection with our assurance engagement, our responsibility is to read the other information and, in doing so, consider whether the other information is materially inconsistent with the description in Section III or our knowledge obtained during the assurance engagement, or otherwise appears to be materially inconsistent or contains a material misstatement of fact. If based on the work we have performed, we conclude that there is a material inconsistency or a material misstatement of fact of this other information, we are required to report that fact. We have nothing to report in this regard.

Intended Users and Purpose

This report and the description of tests of controls in Section VI are intended only for clients 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 clients themselves, when assessing the risks of material misstatements of clients' financial reports/statements.

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, 20 December 2023

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 clients and their auditors with information for their evaluation of the effect of a service organisation on a client's internal control relating to MSWM's internal controls over Private Wealth Management's ("PWM") custody services system throughout the period 1 July 2022 to 30 June 2023.

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 remotely using virtual tools and technologies in Sydney as well as across Asia, the US and UK as well as and onsite visits and in person meetings, where considered necessary. 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 relevant elements of MSWM's control environment as outlined in Section III.

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:
    a) Appropriateness of the purpose of the control and its correlation to the risk/assertion.
    b) Competence and authority of the person(s) performing the control.
    c) Frequency and consistency with which the control is performed.

d) Level of aggregation and predictability.
e) 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 2022 to 30 June 2023. In determining the nature, timing and extent of tests we considered the following:

- Nature and frequency of the controls being tested;
- Types of available evidential matter;
- Nature of the control objectives to be achieved;
- Assessed level of control risk;
- Expected effectiveness of the test; and
- 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:

a) Standard "out of the box" reports as configured within the system;
b) Parameter-driven reports generated by MSWM's systems;
c) Custom-developed reports that are not standard to the application such as scripts, report writers, and queries;
d) Spreadsheets that include relevant information utilised for the performance or testing of a control; and
e) 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 2022 to 30 June 2023. 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 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 in relation to the 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

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 and its affiliates 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 client 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	The PWM General Dealing Terms is part of the Customer Agreement which sets out the Services provided to clients by MSWM and/or MSIP and the terms under which the Services are provided. The Customer Agreement, including the Account Application Form is reviewed by the Account Management Team (AMT) maker after reviewing information provided and entered into PWM New Account Opening (NAO)/ Client Account Management and Onboarding system (CAMO). An AMT manager reviews for completeness and accuracy. From NAO/CAMO the account flows through to PIPE whereby AML/KYC reviews are performed by Client Onboarding Regulatory Service team.	**Inspection** For a sample of new accounts, inspected customer agreements and the account application forms to test whether sign off from AMT was evident. For the sample of new accounts above, inspected whether AML/KYC reviews were performed and signed off in PIPE.	No deviations noted
A.1.B	The set-up of client accounts in the PWM CMS 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 to test whether appropriate review and sign off by a supervisor was performed	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	AMT review and verify the client signatures on the client agreement prior to the account set up being initiated in NAO/CAMO.	**Inspection** Inspected a sample of account opening forms to test whether the signatures on agreements were validated prior to an account being 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 (equity, fixed income, third-party derivative, hedge fund and mutual fund) have been executed by the Financial Adviser, a trade confirmation is automatically generated by the FC3 trade confirmation system and provided to the client.	**Observation** Observed the automatic generation of a trade confirmation after trade details had been entered into the system.	No deviations noted.
A.3.B	Payment and External Asset Transfers Same name external cash payments and asset transfers may be made via a Standing Letter of Authority (SLOA) or a Letter of Authority (LOA). The client signature on the SLOA is verified by the AMT before it is stored in Morgan Stanley's Global Document System (GDS). When requested by the client, a Workflow is created by the front office team who attach the SLOA and submit the request to Operations for payment processing to the client's same name bank account. All third-party payment and asset transfer instructions and same name payment and asset transfers requested via a LOA raised in Workflow are signature verified by Business Unit Risk Management (BURM) before they route to Operations for processing. Where required, in accordance with MSWM Policy, a call-back verification (CBV) is conducted before the payment or asset transfer is released.	**Inspection** Inspected a sample of external cash payment instructions and external asset transfer instructions to test whether checks on letters of authority and signatures were verified by Risk. For a sample of payments and asset transfers, inspected the call back verification to test whether the call back was performed prior to release of payment or asset transfer where required.	No deviations noted

Control Reference	Control Activity	Test Procedures	Results of Tests
A.3.C	There is a segregation of duties when BURM approves and Operations processes payments requests via the Cash Forecasting system.	**Inspection** Observed manual segregation of duties between BURM and Operations. Further, inspected a sample of payment instructions to test whether checks on letters of authority and signatures were verified by BURM. Refer to testing at G.3 for logical separation of access though the Cash Forecasting system.	No deviations noted
A.3.D	A 4 eye check for amounts that are < USD1M and 6 eye check (inputter and 2 authorisers) for amounts > USD1M is completed. Both inputter and authoriser(s) will validate the completeness and accuracy of the instructions.	**Inspection** Inspected a sample of input transactions to test whether review was performed in line with the defined limits to ensure accuracy and completeness according to client instruction.	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	On a daily basis, the Trading Operations – OTC/Cash Settlement team investigates and resolves all Cash/OTC settlement fails captured in the Pari exception queues.	**Inquiry** Inquired with the control owners for each selection to understand the nature of the fails and the control performed for investigating and resolving the fails. **Inspection** For a sample of dates obtained the daily global OTC fails report from the control owners, selected a fail on each report and: (1) inspected email evidence of investigation and communication verifying/corroborating the resolution of settlement fails identified; (2) Inspected SAFE mission showing the break has been properly addressed and resolved within a reasonable time frame.	No deviations noted

Control Reference	Control Activity	Test Procedures	Results of Tests
A.4.B	The settlements reconciliation for OTC derivatives is generated from an automated reconciliation within Pari between Expected Settlements (from Libra) and the Actual Settlements (from SAFE, via Libra).	**Observation** Observed the system owners access the PARI Live Queue tool. **Inspection** 1) Inspected the Live Queue to view the total listing of fails for a sample of dates 2) For the selected sample fails inspected the contractual settlement information in Magnet and traced all relevant attributes to Pari 3) For the selected sample inspected the SAFE Mission to evidence that the actual settlement had not yet occurred and that all the contractual settlement information in SAFE matched what was recorded in Magnet and Pari **Reperformance** For selected samples manually reperformed the Pari reconciliation using the actual and contractual settlement information. **Observation** Observed the system owners access the SAFE settlement system. **Inspection** For the selected sample: 1) inspected the SAFE Mission ID to evidence the actual settlement information 2) inspected Magnet for the contractual (expected) settlement information 3) inspected the Pari reconciliation for the selected account number to determine if the settlement was appropriately matched off or recorded as a fail in the queue.	No deviations noted

Control Reference	Control Activity	Test Procedures	Results of Tests
A.4.C	On a daily basis, the Shared Services & Banking Operations ("SSBO") - Securities Settlement team investigates and resolves all securities settlement fails captured in the SAFE exception queues. Investigations are conducted by notifying and collaborating with relevant stakeholders for resolution. Once the fail has been resolved it will be systematically removed from the live Queue.	**Inquiry** For a sample of dates selected inquired with the control owners to understand the nature of the fails and the control performed for investigating and resolving the fails. **Inspection** (1) For each sample, obtained the daily global secured fails report from the control owners and selected a fail/break on each report. (2) Inspected the evidence where the control owner assess whether MS/Counterparty values or booking was incorrect; (3) Inspected settlement instruction/confirmation from the counterparty/agent bank and inspected the terms of the SAFE mission showing the break has been properly addressed and resolved within a reasonable time frame;	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	Corporate Action Exceptions Asia/Pacific 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 processed or recorded. The team manager reviews this report and ensures exceptions are cleared. Europe/North America Corporate action exceptions from SWIFT are automatically identified on a daily basis by the Scorpio system. Once an action is confirmed, the	**Inspection** Asia/Pacific Inspected a sample of exception reports to test whether breaks were appropriately identified / reported and individually reviewed by the team manager on a timely basis. Europe/North America Inspected a sample of confirmed corporate action exceptions to test whether they were reviewed by a member of the Asset Services Team within Work Items in Scorpio, and prior to event processing all Work Items are reviewed/approved by an independent Asset Services team member.	No deviations noted

Control Reference	Control Activity	Test Procedures	Results of Tests
	exceptions are reviewed by a team member in the Work Items within Scorpio. Prior to event processing all Work Items are reviewed/approved by an independent Asset Services team member.		
A.5.B	Validation of Corporate actions Asset services team validates announcement details in the Scorpio System 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 to test whether they were validated by the Asset Services Team against local custodian and Firm's internal systems before sending the notification to the shareholders.	No deviations noted
A.5.C	Upon payment, Operations reconcile the cash/stock outturn (including investment income) versus an internal calculation and reflect the corporate action (CA) economics in the books and records to ensure no client assets are at risk. An authorisation checklist is completed by Operations to ensure the reconciliation process is completed and breaks are resolved.	**Inspection** Inspected a sample of daily reconciliations between the cash/stock outturn and internal calculation to test whether key positions and payments were properly reconciled and approved, with the CA economics reflected in the books and records. Inspected a sample of authorisation checklists to test whether breaks are followed up and resolved by the Operations team.	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 to test whether execution status and any follow-ups was performed as necessary.	No deviations noted

Control Reference	Control Activity	Test Procedures	Results of Tests
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 to test whether all requests in the system had an associated downstream status and whether a sign off was provided in a report acknowledging completion of task.	No deviations noted

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	*Ongoing reviews are carried out to ensure that a client's investments are in line with pre-determined limits. These limits have been set as part of the client on-boarding process and are based on their risk tolerance and suitability for certain investment types.* The firm's 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. At the end of each week, The KRI report and supervision committee pack is circulated and reviewed by state risk manager.	**Inspection** Inspected a sample of automated e-mails from the CSE system to the Financial adviser, containing breach specifications to test whether a follow up e-mail to the Risk team requiring further action had been sent. Inspected a sample of supervision committee packs to test whether the State Risk Manager monitored the mismatches in a timely manner. Inspected the system configuration to test whether pre and post trade checks were set up appropriately to automatically identify breaches.	No deviations noted
A.10.B	The Compliance team perform quarterly reviews of daily surveillance completed by the offshore surveillance team 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 test 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 Management Inventory system 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 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 financial adviser or CSA, who completes a change request form and submits the form to AMT for approval. For changes that don't require client consent, instructions are communicated through e-mail by AMT. Amendments are done in the system by Operations, after AMT approval.	**Inspection** Inspected a sample of change requests to test whether in each case, a change request form was completed and approved by AMT or e-mail from AMT was sent 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 to test whether it was reviewed and signed off by a supervisor, to ensure changes 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 controls related to Investment Income Recording.
Tax Reclaims - MSWM does not provide a reclaim service for 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	On a daily basis, Morgan Stanley's internal representation of cash balances and stock positions (recorded within LIBRA) are reconciled to statement information received from the Agent and Custodian banks automatically using the Intellimatch reconciliation platform. Intellimatch will automatically generate an exception report with breaks for investigation. Following the performance of the automated control Intellimatch will produce a matched and breaks population, the latter of which is used as the basis for further investigation by business units within Morgan Stanley. The Cash and Stock breaks that are verified through the automated matching are escalated to appropriate business units.	On a sample basis tested combinations of account/currency (for cash) or account/cusip (for stock) from the Intellimatch break report as well as for samples which are not in the Intellimatch break report and tested the automated matching and break functionality in Intellimatch by reperforming the steps for each respective sample selection. For reconciliations: a. Reperformed the transaction matching between the LIBRA and the statement and reconciled with the break report. b. Reperformed the data integrity check between balance and transaction and reconciled with the out of proof report.	No deviations noted
A.13.B	On a daily basis breaks between Morgan Stanley's internally recorded custody balances and the custodians statements are investigated and resolved by the allocated business unit to determine the reason for the break and to perform corrective actions, where necessary, to ensure that the internal representation of cash product positions exist, are complete and that the firm, or the first customers, have the rights to, or obligations of, the positions reported.	Performed inquiries with the control owners (break owner contact) to understand: - the root cause of the break; - how the break owner investigated the break reason; and - whether adjustment to the Morgan Stanley's record was necessary. Inspected a sample of documentary evidence to support the actions taken by the break owner.	No deviations noted
A.13.C	Intellimatch will identify breaks. An email, either Automatic Break Notification ("ABN") from Intellimatch or manually sent from Tata Consulting Service ("TCS") team email application, is sent to the ultimate business owner following identification of that respective Business Unit. The respective ultimate business unit owners will investigate and understand the root cause of the break and any corrective action which needs to take place, or no action is needed. Once fully resolved	Tested breaks on a sample basis across the financial period from AGENTCS Cash report on sample dates. For each sample selection: Inquired to understand - how operations identified the trade to investigation and understand why the trade was unexecuted and steps taken to resolve. - the root cause of the break; - how the break owner investigated the break reason; and	No deviations noted

Control Reference	Control Activity	Test Procedures	Results of Tests
	Intellimatch can be viewed to show the matched status.	- whether an adjustment to the Morgan Stanley's record was necessary. Inspected a sample of documentary evidence to support the actions taken by the break owner.	

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 which are independently reviewed and signed off.	**Inspection** Inspected a sample of Custodian Agreements and Asset Segregation letters to test that to test that these were independently reviewed and signed off.	Not applicable as there were no new custodians onboarded during the period
A.14.B	An annual ongoing due diligence programme is in place, performed by the Network Management team based on which risk ratings are assigned to agent banks, custodian and brokers, holding client money. Morgan Stanley Global Banking Services Due Diligence (GBS DD) performs the desktop due diligence on an annual basis of the credit institution, bank or qualifying money market fund where the money is deposited and on the arrangements for the holding of client money and due diligence reports are prepared and reviewed. The due diligence programme is based on the CASS criteria applicable to MSIP in UK.	**Inspection** Inspected a sample of custodians, banks and brokers' due diligence and risk assessments to test whether they were performed on an annual basis and the reports were reviewed.	No deviations noted

Control Reference	Control Activity	Test Procedures	Results of Tests
A.14.C	On a monthly basis, a report, covering the client money and client assets requirements of CASS is created by the Committee established by EMEA Head of Operations Risk and Regulatory Control ("ORRC") team and included in the monthly Client Assets Governance Committee (CAGC) pack. A member of the IPB Ops team will present this section on monthly CAGC meeting.	**Inspection** Inspected a sample of Client Assets Governance Committee meeting minutes to test whether client money and assets are covered in the meeting.	No deviations noted
A.14.D	Internal and External Reconciliations: Refer to A.13.A to A.13.C for daily reconciliation controls	Refer to A.13.A to A.13.C for 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 BURM 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 BURM, who instructs the Trade Support team to rebook trades as soon as possible.	**Inspection** For a sample of trade errors, inspected the error and rebooking form to test whether sign off/approval by BURM were completed and notifications were sent to trade support for rectification.	No deviations noted
A.16.B	BURM are required to review and provide approval for all cancel and correct requests raised. BURM will provide approval in the workflow system before the request flows to Trade Support to rebook the trade.	**Inspection** Inspected a sample of cancel and correction forms, checked these against the daily reconciliation report, to test whether approval by BURM and instructions were triggered through the workflow system to operations for rectification.	No deviations noted

Control Reference	Control Activity	Test Procedures	Results of Tests
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) to test whether they were signed off by the supervisor and followed up for resolution.	No deviations noted
A.16.D	Internal and External Reconciliations: Refer to control objectives A.4. and A.13 for reconciliation controls over assets and cash.	Refer to Control Objectives A.4 and A.13 for test procedures.	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 appointment and an ad-hoc basis, based on a list of considerations.	**Inquiry** Inquired with management to confirm whether any new custodians for PWM Australia had been appointed within the period. **Inspection** Inspected the Global Network Management team agreement folder to test whether any agreements had been executed within the engagement period. No testing performed, as there were no new subservice relationships during the period.	Not applicable.
A.17.B	MS Global network Management team produce a risk rating annual due diligence report for the custodians and agent banks in question.	**Inspection** Inspected a sample of annual due diligence reports to test whether a risk rating was produced for the custodian/bank in question and whether the due diligence report was signed off by the reviewer to ensure completeness.	No deviations noted

Control Reference	Control Activity	Test Procedures	Results of Tests
A.17.C	Incidents with providers are logged into the Global Incident system and monitored until resolution.	**Inspection** Inspected a sample of incidents to test whether they were recorded and monitored in the Global Incident Network until resolution.	No deviations noted
A17.D	MS Global Network Management team collates a custody and cash clearing provider watchlist to track custodians and agent banks that have an elevated risk rating on a monthly basis. The Country Manager and Regional Head review the watchlist for any elevated risk ratings as well as inclusion/removal of custodians and agent banks on a monthly basis.	**Inspection** Inspected email correspondence of the Country Manager and Regional heads to test whether the review of inclusion/removal of custodians and agent banks and elevated risk ratings was performed.	No deviations noted.

* Internal affiliates are monitored at the Morgan Stanley Global level and the monitoring control is not within the scope of this report or objective.

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 appropriately 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 AUM reports to test whether checks were performed against the official statement, and discrepancies were investigated.	No deviations noted

Control Reference	Control Activity	Test Procedures	Results of Tests
A.18.C	Monthly statement delivery reconciliation is performed to ensure clients receive their online and physical statements. Statement exceptions, if any, are identified and resolved daily until all client statements are sent. A reconciliation is then performed by the Client Reporting Supervisor and signed off on the Renovated Checklist Manager for reconciliation of the monthly statement delivery to the Fuji Film statement.	**Inspection** Inspected a sample of monthly statement delivery reconciliations to test whether physical and electronic statements had been sent to clients during the following month. Inspected the reconciliations to check that exceptions, if any, were identified and resolved. Inspected the Renovated Checklist Manager to test whether the monthly statement delivery reconciliation and Fuji Film statement aligned and was signed off.	No deviations noted

Information Technology

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

Control Reference	Control Activity Description	Test Procedures	Test Results
G1.A	Physical access to data centres is restricted to individuals who require such access to perform their job responsibilities. Data centre access is secured by key card and biometric security systems, and monitored by Corporate Security via video surveillance. Physical access to data centres requires approvals by the designated silo manager and Enterprise Data Centre ("EDC") operations manager. On a quarterly basis, the Enterprise Data Centre ("EDC") operations manager performs a review of users who have card key access to the data centre and ascertains whether their access is commensurate with their job responsibility. On a monthly basis, the EDC operations manager reviews the inactivity report from the key card system and determines whether access is still needed. If not, the access is revoked.	Through inquiry with Enterprise Data Centre operations management and inspection of video surveillance, digital images of the data centre secure access points and in conjunction with biometric security system access logs to capture key card and biometric security activity, ascertained that card key and biometric security systems were used to secure access points and access was monitored by Corporate Security via video surveillance. For a selection of individuals granted access to the data centre, ascertained through inspection of MyBadge logs that user's access was authorised by the designated silo manager and second level approvers. For a selection of quarters, ascertained through inspection of MyBadge logs that the access review was completed by the respective Enterprise Data Centre operations manager and any required access revocations were performed. For a selection of months, ascertained through inspection of the monthly inactive card key review documentation prepared by the EDC Operations manager, that the review was completed and that any required access changes were performed.	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 Description	Test Procedures	Test Results
G2.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.	For the full population of privileged users, inspected the privileged access user listing to the Windows Active Directory network (e.g., Domain administrators) and ascertained that the access was appropriate based on their assigned job roles and responsibility.	No deviations noted.

Control Reference	Control Activity Description	Test Procedures	Test Results
		For a selection Windows servers, inspected the privileged access user listing to the Windows operating system (e.g., Windows Local Administrators) and ascertained that the access was appropriate based on their assigned job roles and responsibility. For the full population of users assigned privileged access to the mainframe, ascertained that the access was appropriate based on their assigned job responsibility within production management. For a selection of Linux servers, inspected the privileged access user listing to the Unix operating system (e.g., users with root access) and ascertained that the access was appropriate based on their assigned job roles and responsibility. For a selection of Linux servers, inspected the security settings for key files to ascertain that access to files is appropriately restricted. For a sample of systems and corresponding databases, inspected the listing of users with privileged access to ascertain the access was appropriate based on their assigned job responsibility within production management.	
G2.B	Access to systems (e.g., network, application, databases, operating systems) require a unique user ID and password. Passwords are implemented to restrict access and are in accordance with the Global Information Security Password Security Procedure.	Through observation with Morgan Stanley Security Administration personnel, ascertained that access to systems (e.g., network, application, databases, operating systems) was restricted through the use of unique User IDs and passwords. Through the inspection of system password policies, ascertained the parameters were defined with minimum password length, password expiration, and password complexity parameters that comply with the Global Information Security Password Security Procedure. For a selection of quarterly password expiration reviews, inspected documentation to ascertain accounts with password expiration set to Not Expire were reviewed and authorised. Discrepancies were monitored, documented and tracked through to resolution.	No deviations noted.

Control Reference	Control Activity Description	Test Procedures	Test Results
G2.C	A Global Technology Security Policy is maintained by the Technology Risk policy management Team. The Global Technology Policy contains requirements for the security of information assets, as well as the necessary standards and procedures to protect such assets for areas such as; identity access management, data security, system and infrastructure security, and network security. The policy and procedures apply to all technology assets and data and are available on the Corporate intranet.	Inspected the Global Technology Security Policy to ascertain that it contained guidance related to security of information assets, identity access management, data security, system and infrastructure security, and network security.	No deviations noted.
G2.D	The identity of remote users is authenticated to the network via a two-factor authentication system. Prior to accessing any system remotely, authentication of the user is verified via an RSA SecurID and the Windows Network Domain Login.	Inspected configuration settings of Production MyDesk servers and ascertained that Active Directory and SecurID authentication policies are enforced. Inspected the system parameters and requirements of the MyDesk system and ascertained that two-factor authentication (e.g. Active Directory and SecurID) is utilised for users to gain remote access.	No deviations noted.
G2.E	Procedures have been established for granting temporary access for technology personnel to the 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") or Secure Temporary Access Privilege ("STAP") request. The TAP/STAP request requires the requestor to enter the purpose of the request, the specific resource for which access is being requested, the length of time access is required, and selection of the role needed. Once the request is entered, TAM utilises a workflow process to route the request to the appropriate resource owner for approval. Once access is approved, the requestor is provided access via TAM with the access automatically revoked once the assigned time period has elapsed.	Through observation with Morgan Stanley Security personnel ascertained that temporary access was managed through the TAM tool via a Temporary Access Privilege (TAP) or Secure Temporary Access Privilege (STAP) request. Through observation with Morgan Stanley Security personnel ascertained that TAP/STAP requests required the requestor to enter the purpose of the request (e.g., emergency, production outage, etc.), the specific resource for which access was being requested, the length of time access was required, and selection of the role needed. Through observation with Morgan Stanley Security personnel ascertained that the role was granted and was revoked automatically once the assigned time had elapsed. For a selection of users granted temporary access, inspected the TAP request and approval	No deviations noted.

Control Reference	Control Activity Description	Test Procedures	Test Results
		documentation to ascertain that the request had the required level of documentation to support the request and was authorised and approved by the appropriate resource owner based on their assigned job responsibility and the revocation of access matched the access requested. For each in-scope STAP infrastructure component, inspected the associated configurations to ascertain that Privileged Access for each technology was appropriately restricted. For a selection of users granted temporary access, inspected the STAP request and approval documentation to ascertain that the request had the required level of documentation to support the request and was authorised and approved by the appropriate resource owner based on their assigned job responsibility and the revocation of access matched the access requested.	
G2.F	For terminations, an automated process exists that removes the user's account (i.e., Windows A/D account, TSS and SecurID) once the Human Resource ("HR") Department updates a personnel's (employee and consultant) status to "terminated" and enters a termination date and last day on premise in the HR system. The Human Resource system sends daily data feeds of newly terminated personnel to the Sun Identity Manager ("SIM"), which then disables all core system accounts (Active Directory, TSS, and SecurID). For the termination of employees, vendors, or contractors which requires urgency, Morgan Stanley utilises the Immediate Access Disablement ("IMAD") process. HR enters the user's information into the SIM tool, which then immediately disables all core system accounts (Active Directory, TSS, and SecurID).	Through observation with Human Resource Department (HR), Windows Active Directory, Sun Identity Manager (SIM), Kerberos and SecurID personnel, ascertained that Workday sent daily data feeds of newly terminated personnel to the Sun Identity Manager (SIM) for systems access disablement of all core system accounts (Active Directory, TSS, and SecurID) based upon termination date and last day on premise. Through observation with Identity and Access Management (IDM) personnel, ascertained the Immediate Access Disablement (IMAD) process utilises SIM to immediately disable all core system accounts (Active Directory, TSS, and SecurID). For a selection of terminated users, ascertained through inspection of the system generated listing of users (i.e., Windows A/D, TSS and SecurID), that user accounts were disabled in a timely manner.	No deviations noted.

G3 - Segregation of incompatible duties is defined, implemented and enforced by logical security controls in accordance with job roles.

Control Reference	Control Activity Description	Test Procedures	Test Results
G3.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.	For the full population of privileged users, inspected the privileged access user listing to the Windows Active Directory network (e.g. Domain Administrators) and ascertained that the access was appropriate based on their assigned job roles and responsibility. For a selection Windows servers, inspected the privileged access user listing to the Windows operating system (e.g., Windows Local Administrators) and ascertained that the access was appropriate based on their assigned job roles and responsibility. For the full population of users assigned privileged access to the mainframe, ascertained that the access was appropriate based on their assigned job responsibility within production management. For a selection of Linux servers, inspected the privileged access user listing to the Linux operating system (e.g., users with root access) and ascertained that the access was appropriate based on their assigned job roles and responsibility. For a selection of Linux servers, inspected the security settings for key files to ascertain that access to files was appropriately restricted. For a sample of systems and corresponding databases, inspected the listing of users with privileged access to ascertain the access was appropriate based on their assigned job responsibility within production management.	No deviations noted.
G3.B	If a user requires access to a Non-WM application, a request needs to be submitted via an access request tool (i.e., GetAccess, Maverick, ServiceNow). The access request tool utilises an automated workflow, to request approval from the appropriate approver (e.g., cost center manager, risk officer). The approver confirms the access is commensurate with the user's job responsibilities. Once approval is obtained, the access request tool programmatically provides the requested	For a selection of users granted access to Non-WM applications, ascertained through inspection of corresponding documentation that the access to the designated application was authorised and approved by appropriate personnel, and the access granted was commensurate with the users' job responsibilities.	No deviations noted.

Control Reference	Control Activity Description	Test Procedures	Test Results
	access, or the access is manually granted by the application admin team.		
G3.C	Access to WM applications and systems is managed via the Entitlements Provisioning and Reporting (EPR) tool. Users are granted an enterprise role based on the user's designated cost center and/ or job code. The enterprise role provides the user access to relevant applications and system entitlements that are aligned with their job responsibilities. If a user requires additional access to WM applications and systems beyond their assigned enterprise role, the user is required to submit a request for the specific entitlement via EPR. EPR utilises an automated workflow to request approval from the appropriate approver (e. g., cost center manager, risk officer) . The approver confirms the access is commensurate with the user's job responsibilities. Once approval is obtained, EPR programmatically provides the requested access.	For a selection of users, ascertained through inspection of the corresponding documentation that the user was granted an enterprise role based on the user's designated cost center and/ or job code. For a selection of users granted application or system entitlements outside of the user's assigned enterprise role, ascertained through the inspection of the corresponding documentation that the access to the designated application or system was approved by an appropriate approver (e. g. , cost center manager, risk officer) , and the access granted was commensurate with the user's job responsibilities.	No deviations noted.
G3.D	User access to applications and systems (e.g., databases, operating systems, network) is reviewed annually by the user's manager or individual(s) nominated by the business unit. The reviews are performed in a centralised access review tool (i.e., Aveksa). Reviewers have the ability to maintain or revoke the user's access, and the reviewer decisions are recorded within the centralised access review tool. The reviews are divided into the following user access review campaigns: • WM Out of Role Review ("OOR") - review of all users with application and relevant system entitlements outside of their assigned enterprise role; • Business Entitlement Review ("BER") – review of all Non-WM users with Non-WM business entitlements; and	Through observation with Morgan Stanley Access Management personnel within Technology & Operations Risk division ascertained that the two entitlement review campaigns (i.e., BER and TER) were performed and completed within the Aveksa entitlement review tool. For a selection of users with access to applications and systems, ascertained through inspection the OOR documentation from Aveksa that the review was completed, and the users' access was reviewed and authorised by the user's manager or individual(s) nominated by the business unit. For a selection of users with access to applications and systems, ascertained through inspection of the BER documentation from Aveksa that the review was completed, and the user's access was reviewed and authorised by the user's manager or individual(s) nominated by the business unit. For a selection of users whose access was revoked as	No deviations noted.

Control Reference	Control Activity Description	Test Procedures	Test Results
	• Technology Entitlement Review ("TER") – review of all users with system entitlements.	part of the review, ascertained through observation and inspection that the users' access in the respective application or system was revoked.	
G3.E	On an annual basis, all active enterprise roles including application and system entitlements assigned to the enterprise roles are reviewed by the enterprise role owner. The reviews are performed in a centralised role review tool (i.e., EPR) where the enterprise role and assigned application and system entitlement data resides. The role owner has the ability to maintain the role with no changes, modify application and system entitlements assigned to a role, or modify the role's metadata (e.g., role owner), or remove the enterprise role. All review decisions are captured within EPR.	Through observation with Morgan Stanley Identity & Access Management personnel within the Cyber Data Risk & Resilience division, ascertained that the enterprise role review was performed and completed within EPR. For a selection of enterprise roles, ascertained through inspection of the EPR review documentation, ascertained the enterprise role was reviewed by the role owner. For a selection of enterprise role changes identified within the enterprise role review, ascertained through observation and inspection that the roles were changed according to the role owner's instructions.	No deviations noted.
G3.F	Privileged user access to systems (e.g., databases, operating systems, network) is reviewed quarterly by the user's manager. The reviews are performed in a centralised access review tool (i.e., Aveksa). Reviewers have the ability to maintain or revoke the user's access, and the reviewer decisions are recorded within the centralised access review tool.	For a sample of quarterly reviews, ascertained through observation with Morgan Stanley Access Management personnel within Cyber Data Risk & Resilience division that the privileged user access review was performed and completed within the Aveksa entitlement review tool. For a selection of privileged users, ascertained through inspection of the quarterly privileged access review documentation from Aveksa that the review was completed, and the users' access was reviewed and authorised by the user's manager. For a selection of users whose access was revoked as part of the review, ascertained through observation and inspection that the users' access in the respective application or system was revoked.	No deviations noted.
G3.G	On a weekly basis, transfer reviews are performed in a centralised access review tool (i.e., Aveksa). Reviewers have the ability to maintain or revoke the user's access, and the reviewer decisions are recorded within the centralised access review tools. Non-WM user transfers will result in the	For a selection of users, ascertained through inspection of the corresponding documentation from EPR, that the user was granted an appropriate enterprise role based on the user's designated job code, cost center and/ or division. For a selection of WM users who changed job codes, cost centers or divisions, inspected the documentation	For the period 1 to 7 July 2022 and 8 September 2022 to 30 June 2023: No deviations noted. For the period 8 July to 7 September 2022:

Control Reference	Control Activity Description	Test Procedures	Test Results
	following actions: • If a user changes job code, cost center, or division the user will be assigned an enterprise role based on their new job code, cost center and/ or division. Relevant WM out of role entitlements of the transferred user automatically marked for revocation. All Non- WM entitlements are reviewed by the user's manager or individual(s) nominated by the business unit. If any entitlements are not reviewed within the defined time, the entitlements are marked for revocation. • If a user changes job code or cost center, the user will be assigned an enterprise role based on their new job code and/ or cost center. Relevant WM out of role entitlements and Non- WM entitlements of the transferred user are reviewed by the user's manager or individual(s) nominated by the business unit. If any entitlements are not reviewed within the defined time, the entitlements are marked for revocation.	from Central Fulfillment Repository (CFR) to ascertain relevant WM out of role entitlements were automatically marked for revocation. Performed an observation with Morgan Stanley Identity & Access Management personnel within the Cyber Data Risk & Resilience division to ascertain transfer reviews were performed and completed within the Aveksa entitlement review tool. For a selection of WM users who changed job codes, cost centers or divisions, inspected transfer review documentation from Aveksa to ascertain the Non- WM entitlements were reviewed by the user's manager or individual(s) nominated by the business unit. For a selection of users whose access was requested to be revoked as part of the review or automatically marked for revocation, ascertained through observation and inspection that the users' access in the respective application or system was revoked.	Deviation noted. For the deviation period above, due to a misconfiguration in the data extraction logic in the entitlement data warehouse, the Information Used in the Control (IUC) for the WM transfer review control was not complete. As a result, certain entitlements for transferred users were not included in the WM transfer reviews being performed by the transferred user's line manager or individuals nominated by business units which could lead to the untimely revocation of entitlements for transferred users. Note: During the deviation period above, the WM weekly transfer reviews were being performed by appropriate management personnel, but due to IUC not being complete, their review was not complete. **Refer to Section VII for Management Response and mitigating controls G3.B, G3.D and G3.F.**
G3.H	On a weekly basis, transfer reviews are performed in a centralised access review tool (i.e., Aveksa). Reviewers have the ability to maintain or revoke the user's access, and the reviewer decisions are recorded within the centralised access review tools. Non-WM user transfers will result in the following actions: • If a user transfers cost center, entitlements of the user are reviewed by the user's manager or individual(s) nominated by the business unit. If any entitlements are not reviewed within the	Performed an observation with Morgan Stanley Access Management personnel within Cyber Data Risk & Resilience division to ascertain transfer reviews were performed and completed within the Aveksa entitlement review tool. For a selection of Non-WM users who transferred divisions, inspected transfer review documentation from Aveksa to ascertain access was automatically marked for revocation. For a selection of Non-WM users who transferred cost center or who transferred division and access revocation was challenged, inspected transfer review	For the period 1 to 7 July 2022 and 8 September 2022 to 30 June 2023: No deviations noted. For the period 8 July to 7 September 2022: Deviation noted. For the deviation period above, due to a misconfiguration in the data extraction logic in the entitlement

Control Reference	Control Activity Description	Test Procedures	Test Results
	defined time, the entitlements are marked for revocation. • If a user transfers divisions, all entitlements are automatically marked for revocation, and individual(s) nominated by the business unit have the ability to review and challenge the revocation. For users whose access revocation was challenged, entitlements of the users are reviewed by the user's manager or individual(s) nominated by the business unit.	documentation from Aveksa to ascertain the review was completed, and the users' access was reviewed by the user's manager or individual(s) nominated by the business unit. For a selection of users whose access was requested to be revoked as part of the review, ascertained through observation and inspection that the users' access in the respective application or system was revoked.	data warehouse, the IUC for the WM transfer review control was not complete. As a result, certain entitlements for transferred users were not included in the WM transfer reviews being performed by the transferred user's line manager or individuals nominated by business units which could lead to the untimely revocation of entitlements for transferred users. Note: During the deviation period above, the WM weekly transfer reviews were being performed by appropriate management personnel, but due to IUC not being complete, their review was not complete. **Refer to Section VII for Management Response and mitigating controls G3.B, G3.D and G3.F.**
G3.I	Access to IT Infrastructure (e.g., operating systems and databases) is controlled via Technology Access Management ("TAM"). Only designated and appropriately secured TAM accounts, as well as production support personnel (e.g., database/ systems administrator) have the ability to access production.	Through observation with Morgan Stanley Security Administration personnel ascertained that access to IT Infrastructure was controlled via Technology Access Management (TAM). For a selection of in scope systems, inspected the infrastructure components (e.g., operating systems and databases) to ascertain TAM was being utilised, and TAM roles were assigned for that system. Obtained a system generated listing of users with TAM access and inspected a sample of users to ascertain access was only granted to production support personnel who required such access as per their assigned job responsibilities.	No deviations noted.
G3.J	Access to distributed systems (e.g., operating system and databases) is managed via the Technology Access Management ("TAM") tool. TAM utilises defined entitlement roles that	Through observation with Morgan Stanley Security personnel ascertained that access to distributed systems (e.g., operating system and databases) was managed	No deviations noted.

Control Reference	Control Activity Description	Test Procedures	Test Results
	provide access to the specific technology resource (e.g., database or operating system). Technology personnel request access via TAM the specific entitlement role needed. The request is then routed to an approver with the appropriate entitlement role for approval. The approver confirms the access is commensurate with the user's job responsibilities. Once approved, the TAM tool will systematically assign the role to the user.	via the Technology Access Management (TAM) tool. Through observation with Morgan Stanley Security personnel ascertained that access to distributed systems required the use of defined entitlement roles that provide access to the specific technology resource (e.g., database or operating system) within TAM. For a selection of TAM access requests to distributed systems, ascertained through inspection of the corresponding documentation that the requests were authorised and approved by an approver with the appropriate entitlement role for approval and the approved role was assigned to the user.	

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

Control Reference	Control Activity Description	Test Procedures	Test Results
G4.A	For the distributed environment automated scheduling tool (i.e., Autosys) is implemented for systems and application processing. Access to the scheduling tools is restricted to production management personnel requiring such access to perform their assigned job responsibility. The automated scheduling tool alerts appropriate teams in the event of errors. Job failures are monitored and resolved by the production management personnel.	For a sample of production Autosys jobs, inspected the job instruction language file to ascertain that production jobs are configured to only allow authorised production management personnel. For a sample of users with access to production Autosys jobs, ascertained that access was appropriate based on their assigned job responsibility within production management. For a selection of production Autosys jobs, inspected the job instruction language file to ascertain that job failure alert settings are configured to alert appropriate teams in the event of errors. For a selection of job failures, ascertained through inspection of ServiceNow tickets, that each alert was monitored by the production management personnel and tracked to resolution.	No deviations noted.
G4.B	Access to update the ISG Mainframe job scheduling tool, Submitor, is restricted to production management personnel required to perform their assigned job roles and responsibilities.	For the full population of privileged users with access to the Submitor job scheduler, ascertained that access was authorised to production management personnel and consistent with their assigned job roles and responsibilities.	No deviations noted.

Control Reference	Control Activity Description	Test Procedures	Test Results
G4.C	Job monitoring is performed by the ISG Data Center utilising Problem Report Facility Dashboard for Submitor job abends. In the event of a job failure, designated stakeholders (e.g. Production Management, Mainframe Scheduling and Application Owner) are notified of the issue via a ServiceNow ticket where issues are tracked to resolution.	For a selection of Submitor abends, inspected the Submitor Job History to ascertain that either the Job was successfully rerun by operations personnel, or the incident was escalated to ServiceNow ticketing system. For those instances that were escalated, inspected the corresponding ServiceNow tickets to ascertain that each incident was acknowledged by technology personnel and tracked to resolution.	No deviations noted.
G4.D	For all changes executed through ADHOC (used to initiate one-time jobs that do not previously exist in the scheduler), Production Management (PM) and Mainframe Computing Data Center (DC) approvals are required in the system prior to execution to the production environment.	For a selection of ADHOC Jobs, ascertained through inspection of the documentation that requests were approved by authorised individuals prior to job being executed into production environment.	No deviations noted.
G4.E	For all changes executed through DCRQ (used for one time out of schedule changes made to existing production jobs), Production Management (PM) and Mainframe Computing Data Center (DC) approvals are required in the system prior to execution to the production environment.	For a selection of DCRQ requests, ascertained through inspection of the documentation, that requests were approved by authorised individuals prior to job being executed into production environment.	No deviations noted.
G4.F	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 ServiceNow ticketing systems and are tracked to resolution. On a weekly basis, Weekly Incident Management Review Meetings (WIRM) are conducted by the Enterprise Command Center (ECC), which is a part of the Enterprise Technology & Services (ETS) division, to review and track resolved firm wide technology incidents that are categorised with a business impact of S1- Severe, S2 – Major, or S3/4 – Near Miss. The review determines the accountability and ownership of these incidents and their associated problems.	For a selection of incidents, ascertained through inspection of ServiceNow tickets that each incident was acknowledged by technology personnel and tracked to resolution. For a selection of S1, S2, and S3/4 incidents, ascertained through inspection of Weekly Incident Management Review Meeting (WIRM) minutes that incidents were discussed and documented during WIRM meetings, and that the root cause/owner were identified.	No deviations noted.

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

Control Reference	Control Activity Description	Test Procedures	Test Results
G5.A	Firewalls are utilised to restrict incoming and outgoing traffic from external networks. Intrusion detection systems are implemented at key points throughout the network to monitor suspicious traffic. Alerts are monitored by the MSSOC (Security Operations Center) and escalated to MSCIRT (Cyber Incident Response Team) for investigation and potential remediation.	Through inquiry and observation with Morgan Stanley Security personnel ascertained that firewalls to restrict traffic and intrusion detection systems were utilised within the Morgan Stanley IT environment. For a selection of incidents, ascertained through inspection of corresponding tickets, that each incident was monitored and tracked to resolution by the MSSOC and MSCIRT.	No deviations noted.

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

Control Reference	Control Activity Description	Test Procedures	Test Results
G6.A	Data centers have independent air conditioning systems, humidity and temperature controls, smoke and fire detection, and fire suppression systems. Data centers 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 center are monitored through local and centralised monitoring stations.	Through inquiry with Enterprise Data Center operations management, ascertained that environmental protection measures are in place to ensure availability of IT resources. Through observation and inspection of digital images and maintenance logs of independent air conditioning systems, humidity and temperature control, smoke and fire detection, and fire suppression systems within the data centers, ascertained the existence of independent air conditioning systems, humidity and temperature control, smoke and fire detection, and fire suppression systems. Through observation and inspection of digital images and maintenance logs of surge protectors, power supplies and generators within the data centers, ascertained the existence of surge protectors, power supplies, and generators to protect IT resources in the event of a power disruption. Through observation and inspection of digital images and maintenance logs of environmental control systems within the data centers, ascertained the environmental control systems are monitored through local and	No deviations noted.

Control Reference	Control Activity Description	Test Procedures	Test Results
		centralised monitoring stations.	

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.

Control Reference	Control Activity Description	Test Procedures	Test Results
G7.A	Applications within the distributed environment have their code and other files maintained within Perforce or Git. Perforce and Git are version management systems that track and provide controls over changes to source code. It provides the option to lock files or allow simultaneous changes of files with the ability to merge such changes into one final version. Access to "check out" and "check in" changes for each application is restricted to appropriate personnel responsible for application development.	Through observation with Morgan Stanley Change Management personnel, ascertained that source code and other file-based artifacts were maintained within Perforce and Git for applications on the distributed platform. Through observation with Morgan Stanley technology personnel, ascertained that Perforce and Git allows simultaneous changes of files with the ability to merge such changes into one final version. Through inspection of a system generated listing of users with the ability to "check out" and "check in" files within the Perforce and Gitversion management tools, ascertained that access was authorised to application development personnel and consistent with assigned job roles and responsibilities.	No deviations noted.
G7.B	Application and Database changes to the Morgan Stanley's distributed environment are documented, tested, and approved prior to implementation into production. The distributed environment utilises automated tools (i.e., VMS, Autosys, DB2TS, SYTS and Runway) 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	Through observation with Morgan Stanley Change Management personnel, ascertained that the distributed environment utilised automated change tools to migrate changes into production and changes 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. 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. 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 Description	Test Procedures	Test Results
	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.		
G7.C	A turnover to the distributed environment can be moved into production without an approved TCM in cases of emergencies. 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 for their assigned application according to policy. Late signoffs to emergency changes are monitored by Technology Risk Committee (TRC) and reported via the Top 30 (T30) Risk Metrics during the TRC monthly meetings. If the total number of emergency changes exceed the minimum threshold defined in the T30, developers are required to provide additional rationale for each change to be included in the T30 commentary and shared with senior management.	For a selection of emergency changes in the distributed environment, ascertained through inspection of the documentation, that late-signoffs were monitored, commentary and rationale were shared in the meeting, and the change was reviewed through resolution during monthly TRC meetings. For a selection of TRC meetings, ascertained through inspection of meeting minutes, (where attendees were logged, meeting focus areas and agenda topics were included, and emergency changes reviewed) that management monitored the use of emergency changes that exceeded the defined minimum threshold and provided additional rationale that was shared with senior management.	No deviations noted.
G7.D	Infrastructure system changes (e.g., network, operating system, firewall) to the distributed and mainframe environment are documented and approved prior to implementation into production.	For a selection of infrastructure changes (i.e., network, operating system, firewall) to the distributed and ISG mainframe environment, ascertained through inspection of the change documentation that the changes were documented and approved prior to implementation into production.	No deviations noted.
G7.E	Applications within the Non-WM Mainframe production environment have their source code maintained within CM Suite. CM Suite is a version management system that tracks and provides controls over changes to source code.	Through observation with Morgan Stanley Change Management personnel, ascertained that source code were maintained within CM Suite for applications on the Non-WM Mainframe environment. Through observation of CM Suite, ascertained that CM Suite enables users to lock or unlock files when editing a code to allow multiple developers to work on the same piece of code without overriding the existing code.	No deviations noted.
G7.F	Changes to Non-WM mainframe environment (applications, databases, and jobs) are	For a selection of ICUA changes (i.e., applications, databases, and jobs) to the mainframe environment,	No deviations noted.

Control Reference	Control Activity Description	Test Procedures	Test Results
	documented, tested, and approved prior to implementation into production. The Non-WM mainframe environment utilises automated tools (i.e., ICUA and FMOD) together with Technology Change Management (TCM) to migrate changes into production. In order to migrate a change into production, the turnover tools require an approved Technology TCM ticket.	ascertained through inspection of the change documentation that the changes were documented, aligned with TCM tickets, which include testing and approval information, and approved prior to implementation into production. For a selection of FMOD changes (i.e., databases) to the mainframe environment, ascertained through inspection of the change documentation that the changes were documented, aligned with TCM tickets, which include testing and approval information, and approved prior to implementation into production.	

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

Control Reference	Control Activity Description	Test Procedures	Test Results
G8.A	Management approves the results of the conversion of data from the old application system or data structure to the new application system or data structure and monitors that the conversion is performed in accordance with established conversion policies and procedures.	Through inquiry with IT System Owners and Risk Officers, ascertained there were no data migration or modifications to the in-scope applications during the examination period. Further corroborated during testing of in scope applications that no data migrations or modifications occurred.	There were no occurrences of data migration or modifications to the in-scope applications during the period.

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

Control Reference	Control Activity Description	Test Procedures	Test Results
G9.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.	Through multiple observations with Morgan Stanley Enterprise Infrastructure personnel, Ascertained that an automated tool is used to perform daily / weekly backups according to Company policy. For a selection of servers, ascertained through inspection of Enterprise Server Platform (ESP) that incremental backups were performed daily and full backups were performed weekly. For a selection of backup failures, ascertained through inspection of ServiceNow tickets that full and incremental backup processes were monitored and errors were tracked to resolution by the production	No deviations noted.

Control Reference	Control Activity Description	Test Procedures	Test Results
		support team in a timely manner based on business requirements. Inspected mainframe backup job configurations to ascertain that daily incremental and weekly full backups were configured according to Company policy. For a selection of mainframe backup abends, inspected documentation to ascertain that failures were tracked and resolved by the production support team.	

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

Control Reference	Control Reference	Control Reference	Test Results
G10.A	Please refer to G4.A, G4.C, and G4.F above for control activities identified above to achieve G10.	Please refer to G4.A, G4.C, and G4.F above for control activities identified above to achieve G10.	No deviations noted.

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

Control Reference	Control Reference	Control Reference	Test Results
G11.A	The 'Global Technology Disaster Recovery Procedure' defines the disaster recovery testing frequency and tier mapping of applications for Technical Recovery Plans (TRP) of firm assets. Disaster recovery tests are conducted in accordance with the frequencies defined in the 'Global Technology Disaster Recovery Procedure'. Technical Recovery Plans (inclusive of Business Continuity Plans) are reviewed and signed off by appropriate personnel as defined in the governing 'Global Technology Disaster Recovery Procedure'.	Obtained and inspected the 'Global Technology Disaster Recovery Procedure' to ascertain the frequency of disaster recovery testing and tier mapping of applications for TRPs were defined in the governing policy. Inspected disaster recovery test results for a sample of applications to ascertain that the application was tested in accordance with the frequencies defined in the 'Global Technology Disaster Recovery Procedure'. Inspected the TRPs for a sample of applications to ascertain that the TRP was reviewed and signed off by appropriate personnel in accordance with 'Global Technology Disaster Recovery Procedure'.	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 MSWM to provide additional information to clients 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:

CO Ref	Control Activity	Deviation Noted	Management Response
G3.G	On a weekly basis, transfer reviews are performed in a centralised access review tool (i.e., Aveksa). Reviewers have the ability to maintain or revoke the user's access, and the reviewer decisions are recorded within the centralised access review tools. Non-WM user transfers will result in the following actions: • If a user changes job code, cost centre, or division the user will be assigned an enterprise role based on their new job code, cost centre and/ or division. Relevant WM out of role entitlements of the transferred user automatically marked for revocation. All Non- WM entitlements are reviewed by the user's manager or individual(s) nominated by the business unit. If any entitlements are not reviewed within the defined	For the period 8 July to 7 September 2022: Deviation noted. For the deviation period above, due to a misconfiguration in the data extraction logic in the entitlement data warehouse, the IUC for the WM transfer review control was not complete. As a result, certain entitlements for transferred users were not included in the WM transfer reviews being performed by the transferred user's line manager or individuals nominated by business units which could lead to the untimely revocation of entitlements for transferred users. Note: During the deviation period above, the WM weekly transfer reviews were being performed by appropriate management personnel, but due to IUC not being complete, their review was not complete. **Mitigating Controls:** G3.D User access to applications and systems (e.g., databases, operating	Management self-identified the misconfiguration in the data extraction logic within the entitlement datawarehouse, and acknowledges that a subset of entitlements were excluded from the non-WM transfer review control. Management has confirmed that the entitlement datawarehouse misconfiguration has been remediated. Management noted the risk of inappropriate access upon transfer was addressed through the effective detective controls (i.e., BER and OOR) that were initiated after the entitlement datawarehouse

CO Ref	Control Activity	Deviation Noted	Management Response
	time, the entitlements are marked for revocation. • If a user changes job code or cost centre, the user will be assigned an enterprise role based on their new job code and/ or cost centre. Relevant WM out of role entitlements and Non- WM entitlements of the transferred user are reviewed by the user's manager or individual(s) nominated by the business unit. If any entitlements are not reviewed within the defined time, the entitlements are marked for revocation.	systems) is reviewed annually by the user's manager or individual(s) nominated by the business unit. The reviews are performed in a centralized access review tool (i.e., Aveksa). Reviewers have the ability to maintain or revoke the user's access, and the reviewer decisions are recorded within the centralized access review tool. The reviews are divided into the following user access review campaigns: • WM Out of Role Review ("OOR") – review of all users with application and relevant system entitlements outside of their assigned enterprise role; • Business Entitlement Review ("BER") – review of all Non-WM users with Non-WM business entitlements; and • Technology Entitlement Review ("TER") – review of all users with system entitlements. Additionally, MS has other preventative controls G3.B (i.e., new user access) and G2.F (i.e., termination control) to ensure that each time a user gets access to an in-scope system, its documented and authorized prior to implementation, and terminated user access is revoked timely. Further, MS has periodic access review controls (i.e., G3.D – TER (see above), and G3.F – Privileged Access Review) to ensure user's access is appropriate during their employment at MS. Management and D&T identified these preventative and detective controls as additional mitigating controls, and these controls collectively address the GS007 Guidance Statement Requirement, documented in column 'C'.	misconfiguration was remediated.
G3.H	On a weekly basis, transfer reviews are performed in a centralised access review tool (i.e., Aveksa). Reviewers have the ability to maintain or revoke the user's access, and the reviewer decisions are recorded within the centralised access review tools. Non-WM user transfers will result in the following actions: • If a user transfers cost centre, entitlements of the user are reviewed by the user's manager or individual(s) nominated by the business unit. If any entitlements are not reviewed within the defined time, the entitlements are marked for revocation. • • If a user transfers divisions, all entitlements are automatically marked for revocation, and individual(s) nominated by the business unit have the ability to review and challenge the revocation. For users whose access revocation was challenged, entitlements of the users are reviewed by the user's manager or individual(s) nominated by the business unit.	G3.B If a user requires access to a Non-WM application, a request needs to be submitted via an access request tool (i.e., GetAccess, Maverick, ServiceNow). The access request tool utilizes an automated workflow to request approval from the appropriate approver (e.g., cost centre manager, risk officer). The approver confirms the access is commensurate with the user's job responsibilities. Once approval is obtained, the access request tool programmatically provides the requested access, or the access is manually granted by the application admin team. G2.F For terminations, an automated process exists that removes the user's account (i.e., Windows A/D account, TSS, and SecurID) once the Human Resource ("HR") Department updates a personnel's (employee and consultant) status to "terminated" and enters a termination date and last	

CO Ref	Control Activity	Deviation Noted	Management Response
		day on premise in the HR system. The Human Resource system sends daily data feeds of newly terminated personnel to the Sun Identity Manager ("SIM"), which then disables all core system accounts (Active Directory, TSS, and SecurID). For the termination of employees, vendors, or contractors which requires urgency, Morgan Stanley utilizes the Immediate Access Disablement ("IMAD") process. HR enters the user's information into the SIM tool, which then immediately disables all core system accounts (Active Directory, TSS, and SecurID). G3.F Privileged user access to systems (e.g., databases, operating systems, network) is reviewed quarterly by the user's manager. The reviews are performed in a centralized access review tool (i.e., Aveksa). Reviewers have the ability to maintain or revoke the user's access, and the reviewer decisions are recorded within the centralized access review tool.	