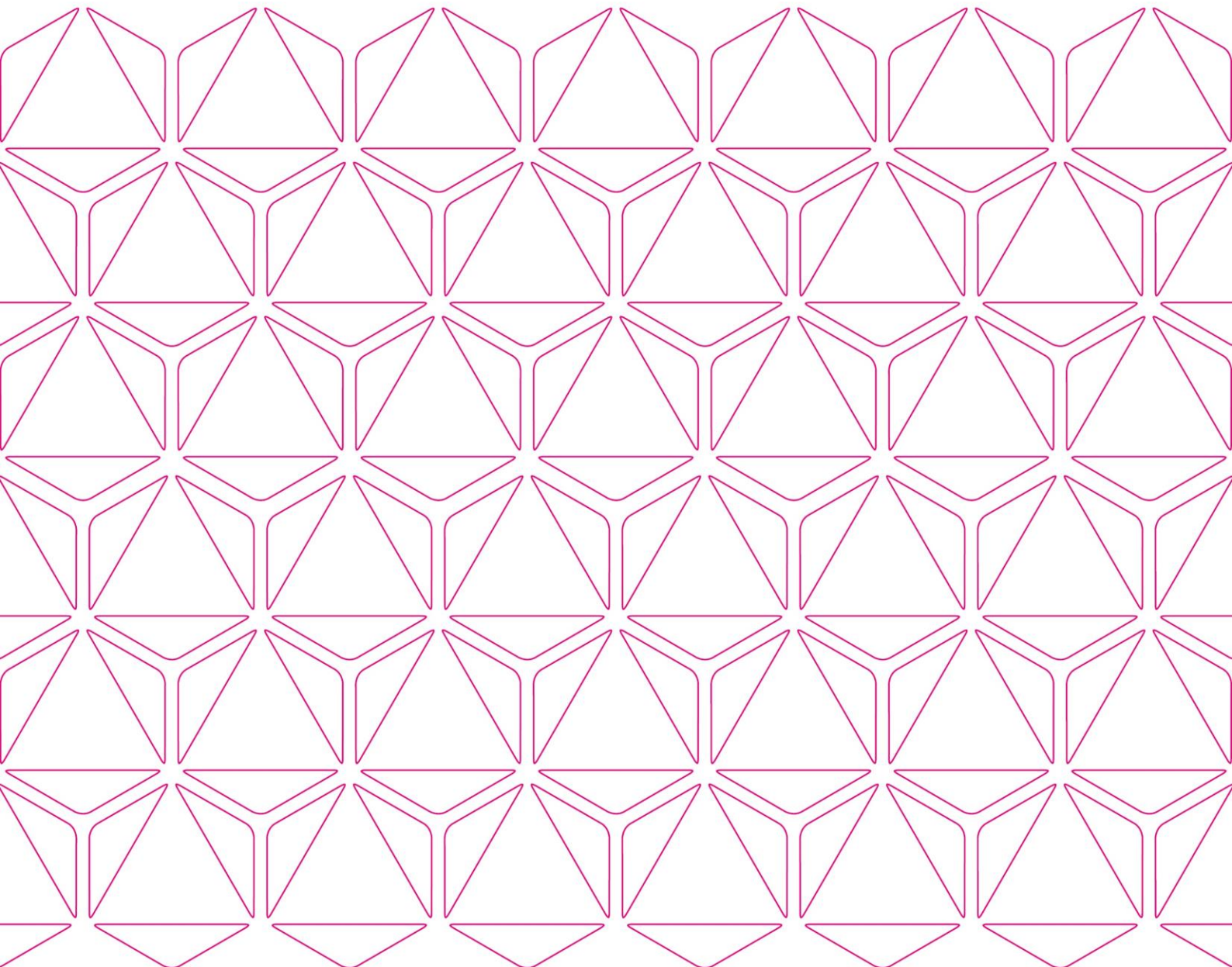


Independent Service Auditor's Assurance Report on the Description of Controls, their Design and Operating Effectiveness for the Praemium portfolio administration application

1 July 2022 – 30 June 2023



Contents

1.	Report of Independent Service Auditors	3
2.	Management's Assertion	6
3.	Praemium Limited's Description of System and Controls	7
4.	The Company's Controls and Testing Performed by the Service Auditor	16
5.	Other information not covered by the Auditor's report	57

1. Report of Independent Service Auditors

10 August 2023

To the Management and the Board of Directors of Praemium Limited:

Scope

We have been engaged to report on the control environment as set out in the accompanying description of Praemium Limited's ("Praemium" or "the Company") controls relating to the provision of its VMA Application, for the period 1 July 2022 to 30 June 2023 ("Specified Period") in order to express an opinion about the design and effectiveness of these controls based on the description of the control objectives detailed in Section 3 of this report ("the Description").

Praemium uses managed service providers for some of its datacentre management and application support services. The Description in Section 3 includes only the control objectives and related controls of Praemium and excludes the control objectives and related controls of the managed service providers. Our examination did not extend to controls of the managed service provider(s) and we have not evaluated the suitability of the design or operating effectiveness of such subservice organisation controls.

Praemium's Responsibilities

Praemium is responsible for preparing the description of controls contained in Section 3, 'Praemium Limited's Description of its Systems and Controls', including the completeness, accuracy and method of presentation, and maintaining an effective internal control structure including control procedures in relation to the provision of the Praemium Portfolio Administration Application ("Praemium VMA Application").

Management's assertion on the design and effectiveness of the internal controls in relation to the Praemium Application is included in Section 2, 'Management's Assertion'.

Our Independence and Quality Control

We have complied with the relevant ethical requirements relating to assurance engagements, which include independence and other requirements founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

In accordance with Auditing Standard ASQM 1 *Quality Management for Firms that Perform Audits or Reviews of Financial Reports and Other Financial Information, or Other Assurance or Related Services Engagements*, Grant Thornton Audit Pty Limited (Grant Thornton) maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Service Auditor's Responsibilities

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

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 Company's Description, 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. Our procedures included testing the design and operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the Description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the Description, the suitability of the objectives stated therein, and the suitability of the Description specified by the Company and described in Section 3.

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

Limitations of Controls at a Service Organisation

Praemium's Description is prepared to meet the requirements of Praemium's clients and their auditors, and may not, therefore, include every aspect of the system that each user of the report may consider important in their own particular environment.

Also, because of their nature, controls at a service organisation may not prevent all or detect all errors or omissions in processing or reporting transactions.

Opinion

Our opinion has been formed on the basis of the matters outlined in this report. The criteria we used in forming our opinion are those described at Sections 2 and 3. In our opinion, in all material respects:

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

Description of Tests of Controls

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

Intended Users and Purpose

This report is intended only for customers who use the Praemium application, and their auditors, who have a sufficient understanding to consider it, along with other information including information about controls operated by customers themselves, when obtaining an understanding of customers' information systems relevant to financial reporting.

GRANT THORNTON AUDIT PTY LTD



Matthew Green
Partner – Risk Consulting




Darren Scammell
Partner – Audit & Assurance

2. Management's Assertion

The accompanying description has been prepared for customers who have used the Praemium portfolio administration application and their auditors who have a sufficient understanding to consider the description, along with other information including information about controls operated by customers themselves, when obtaining an understanding of customers' information systems relevant to financial reporting. Praemium Limited confirms that:

1. The accompanying description, Section 3, fairly presents the Praemium portfolio administration application for the period 1 July 2022 to 30 June 2023. The criteria used in making this assertion were that the accompanying description:
 - i. Presents how the system was designed and implemented, including:
 - The types of services provided, including, as appropriate, classes of transactions processed.
 - The procedures, within both information technology and manual systems, by which those transactions were initiated, recorded, processed, corrected as necessary, and transferred to the reports prepared for customers.
 - The related accounting records, supporting information and specific accounts that were used to initiate, record, process and report transactions; this includes the correction of incorrect information and how information was transferred to the reports prepared for customers.
 - How the system dealt with significant events and conditions, other than transactions.
 - The process used to prepare reports for customers.
 - Relevant control objectives and controls designed to achieve those objectives.
 - Controls that we assumed, in the design of the system, would be implemented by customers, and which, if necessary to achieve control objectives stated in the accompanying description, are identified in the description along with the specific control objectives that cannot be achieved by ourselves alone.
 - Other aspects of our control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls that were relevant to processing and reporting customers' transactions.
 - ii. Includes relevant details of changes to the service organisation's system during the period 1 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 customers and their auditors and may not, therefore, include every aspect of the system that each individual customer may consider important in its own particular environment.
- b) The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period 1 July 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 would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved; and
 - iii. The controls were consistently applied as designed, including that manual controls were applied by individuals who have the appropriate competence and authority, throughout the period 1 July 2022 to 30 June 2023.

Sincerely


David Coulter, Aug 2, 2023 14:29 GMT+10

David Coulter
CFO - Praemium Limited

2 August 2023

3. Praemium Limited's Description of System and Controls

Overview

This report has been prepared to provide background and information applicable to the controls and procedures implemented by Praemium Australia Ltd ("Praemium"), relating to its' VMA product and the report is provided to Praemium's clients who require such an audit to be undertaken.

The company

Praemium was founded in Australia in October 2001 and was formed to provide a web-based portfolio administration service, branded VMA, to professional adviser clientele to administer investment portfolios. Its' niche was specialised corporate action management and investment tax reporting under their own label for multiple portfolios across their own client base. In 2005 the SMA technology was developed, leveraging the VMA functionality. This incorporated automated rebalancing to managed investment portfolios, allowing scalability and customisation for individual investor needs.

In May 2006, Praemium listed on the Australian Stock Exchange with the specific intent of raising funds to finance expansion in Australia and to establish a UK operation. Following success in the UK with running an SMA platform, in late 2012, Praemium expanded its' Australian business by fully acquiring the BlackRock SMA. The BlackRock SMA utilised Praemium's technology, so the purchase was complementary and enabled Praemium to become the Responsible Entity and operator of the registered managed investment scheme thus providing an Australian version of a similar fully administered custody solution.

In the same year, Praemium acquired Wealthcraft Systems Limited which expanded its product suite to provide integrated CRM services and financial planning tools. Praemium entered the UK market in 2015-2016 and established businesses in Hong Kong and China. After a review of these businesses, they were divested to enable Praemium to focus on increasing market share in Australia.

In October 2020, Praemium completed the off-market takeover of Powerwrap Limited, one of Australia's leading wealth management platforms. Powerwrap offers a comprehensive suite of investment, administration, and shared services to high-net-worth investors, with a broad range of investments and comprehensive set of administration and reporting tools for portfolio management. The addition of Powerwrap, which already utilised Praemium's core technology, positioned Praemium to deliver a holistic wealth management solution on a single platform.

Corporate structure

The Praemium group of companies comprises Praemium Limited, the Australian listed entity, (ASX: PPS), Praemium Australia Limited, the Australian operating entity for Wrap and the SMA, (which holds AFS Licence 297956), Powerwrap Limited (which holds AFS Licence 329829), MWH Capital (which holds AFS Licence 338141) and Praemium RA LLC (which provides administration and technology support to Praemium, located in Armenia).

As at June 2023, in addition to non-executive directors, Praemium employed 259 people in its Australian operations and 342 overall.

Oversight by the board of directors

At 30 June 2023 the parent company, Praemium Limited, had a Board of four non-executive directors and the Managing Director. There are two committees, which report to Praemium Limited's Board, comprising various members of the Board and each chaired by a Non-Executive Director:

- Audit, Risk & Compliance Committee; and
- Remuneration & Nomination Committee.

The Board and each Committee operates under Charters approved by the Board.

The Board has also adopted a corporate governance and code of conduct framework by which all entities within the group operate to the extent possible under applicable jurisdictions' law and regulatory requirements. This provides guidance for the Board and all employees in defining their roles, responsibilities and conduct. It also assists the company in complying with its regulatory and legislative requirements.

The Australian operating company, Praemium Australia Limited, also had a Board, comprising 3 executive directors. This Board is augmented with a senior management team for decisions on operating strategy, compliance and risk management and product development.

Policies, standards and procedures

Praemium has a comprehensive framework of policies which are regularly reviewed and presented to the Board for approval. These policies are supported by a number of procedures and checklists.

In addition, there are IT Disaster Recovery (DRP) and Business Continuity Plans (BCP) which are tested at least annually and a Risk Management Plan with a register that aligns with Standard AS4360.

The services

VMA is delivered to clients via internet and browser technologies. It is fully supported by IT Development and technical support teams and operational support which include personnel who manage the onboarding processes, corporate actions processing and Security pricing as well as client query resolution.

VMA

VMA is a branded online portfolio administration service designed for various types of professional investment managers. It has a capital gains tax (CGT) processing and reporting capability designed to optimise CGT calculations for all tax entity types.

VMA accepts data feeds of a large range of assets including ASX and international equity trades, options and, where available, CHESS movements and holdings at its clients' discretion and in various formats. Praemium undertakes to upload these into investor portfolios daily. It also provides daily pricing information for assets where pricing feeds are available, driven by client demand. A facility is available for users to maintain, update and price other assets they may have in order to provide tax management over all assets owned including Fixed Interest instruments.

VMA overlays corporate actions based on the portfolio holdings and reconstructs portfolios as the underlying holdings change, by systematically removing all existing corporate action information and tax calculations and then reconstructing every time a portfolio is recalculated. This can be done manually but is also done overnight for all active portfolios in the system, thus keeping portfolios fully up to date.

Alongside this, Praemium has the ability to record cash transactions from a selection of banking institutions via file feeds or as a manual function. It provides a comprehensive range of transaction, tax and performance reports which can be selected to create client report packs.

These reports are available via the website for clients and their nominated representatives.

VMAAS

The VMA Administration Service is an add-on to the Praemium VMA that enables financial planning practices to outsource the administration of their client portfolios to Praemium, freeing up advisers from the time-consuming tasks associated with managing clients' investment portfolios.

Managing non-custodial client assets directly in a HIN-based structure is a popular option for advisers, especially for their higher-value clients, but can become a substantial administration burden. Adding full administration support – from mail house, portfolio management, account reconciliation, corporate action election processing through to full annual reporting – makes the HIN-based managed account a more attractive option. VMAAS can also be combined with Praemium's Managed Accounts platform for professional investment management and reporting. VMAAS is an important addition to Praemium's Integrated Managed Accounts Platform as it enables advisers to serve their clients' administration and investment needs from a single platform.

The processes the VMA Administration team performs for advisers are as follows:

Mail House Services

Praemium receives all clients mail via a dedicated post box. Our service then receipts and processes the mail, stores all documents securely and provides access to this mail on request.

Portfolio Management

Praemium performs all the administration tasks required to fully reconcile client portfolios including transaction matching and investigating and resolving unreconciled items.

Any information gaps are resolved via interaction with key service contacts at each client.

Praemium Corporate Action Election Processing

Praemium identifies all portfolios impacted by a Corporate Action and notifies the adviser via the Corporate Action Notification tool on Adviser Portal.

Advisers place eligible Corporate Action Elections via Adviser Portal and Praemium will update the investors account based on the adviser's election. All the non-compulsory CAs have been managed via the tool since 1 July 2021

Praemium Corporate Action Election Execution File Preparation

Once all Corporate Election decisions have been received from clients, Praemium prepare a bulk payment instruction file for the client to execute.

Praemium will work with each client to determine the execution and settlement process the client would like to implement.

Fee Generation

Praemium generate client fee invoices on behalf of the financial adviser using the Praemium system on a monthly or quarterly basis and confirm with adviser.

Monthly or Quarterly Reporting (additional fee)

Praemium run standard reports on a Monthly or Quarterly basis and provide to clients via SFTP or via Praemium's Investor Portal.

Annual Tax Reporting

Praemium prepare and generate annual tax reports on behalf of clients.

Reports are provided to clients via direct download, SFTP or via Praemium's Investor Portal.

Reconciliation frequency

Reconciliation frequency is agreed with clients and generally Australian equities, managed funds, CMAs with automated data feeds will be reconciled daily, and all other asset types are reconciled monthly.

Description of IT

The control objectives and related controls listed in Section 4 of this report relate to the following IT systems:

Infrastructure

The Praemium application and related services are delivered through a web-based experience. This has been designed, built and operated for performance, redundancy and security, at the physical, logical and process layers.

The physical environment utilises best of breed data-centre facilities provided by a third-party, with sites currently located in Melbourne and Sydney for geographic redundancy. The physical aspects of the system design are built for redundancy, availability and operational security and monitoring.

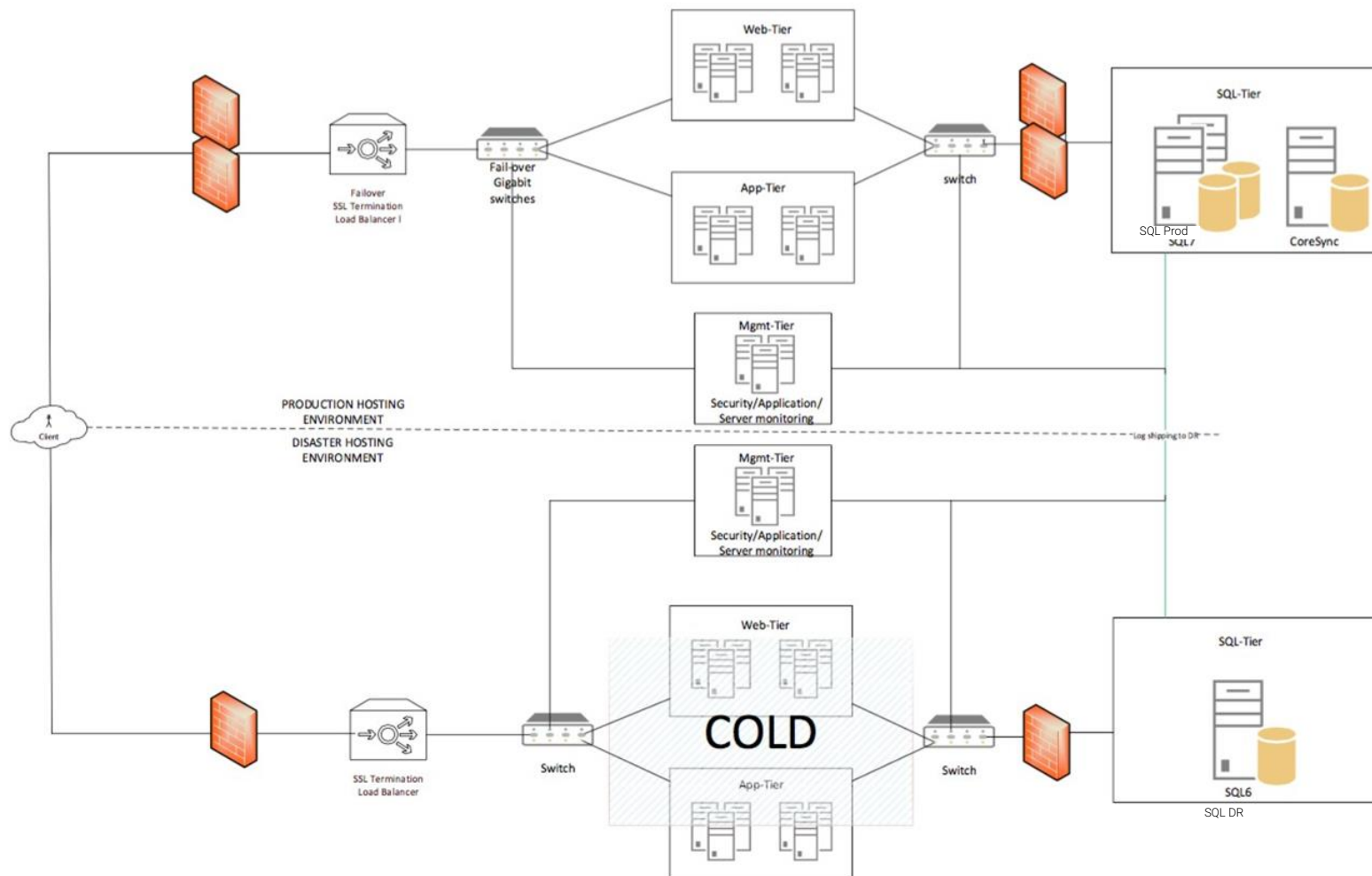
These data centre environments are augmented with the use of public cloud, via Microsoft Azure, an ISO27001 certified operating environment, again with resources located in Melbourne and Sydney, along with specifically chosen international locations for broader redundancy.

The logical and operating processes are structured to ensure integrity and confidentiality across our software, systems and data, following many principles such as least-privilege and defence-in-depth.

The following strategies have been adopted by Praemium to ensure that access to reliable computing and application infrastructure is available to deliver critical business functions:

- Use of purpose-built data centres with environmental controls and physical security hosted by a third party provider
- Multiple network paths for content delivery and inter-site connectivity
- High-availability design of critical systems, firewalls and components
- Consideration of physical and logical isolation based on data classification
- Internally built and managed server environment
- High speed data transfer and synchronisation to various sites
- Monitoring of system performance and incident-awareness through in-house monitoring applications and off the shelf software products.
- Formal patch-management monitoring and application processes
- Formal software change-management processes with quality assurance and oversight
- Testing of disaster recovery procedures

A high-level infrastructure diagram is provided below.



IT Processes

Restricting access to systems and data

Access to systems and data is limited to users on an as-needed basis, is segregated by role, is requested and approved through a managed process, is only provided after sufficient training has been undertaken and is reviewed regularly. Access to production environments is additionally controlled on a responsibilities basis where a multi-tiered support functions exist, with the primary support function acquiring read-only access. Access to systems and data is approved on a permanent basis for those who require it to fulfil their role and duties (i.e. Release Managers). Those with heightened access to the application (i.e. Level 13 User) are trained and approved through a managed process. All support administrator (Level 13 access) access is reviewed by management on a monthly basis and actioned if necessary. Non-production environments only contain cleansed data, conducted automatically as part of database restoration processes.

A number of mechanisms are utilised to capture changes made to specific data, including changes made through the front-end application and any back-end data maintenance or software updates where these may modify specific data. This specific data is deemed critical by the business and may include bank accounts, user information and other data which we deem important. Changes to such data are captured and stored indefinitely, and this provides a path to review changes and the persons who made the changes, providing the opportunity for forensic review if required.

Authorising and processing transactions

Transaction processing occurs automatically as part of the underlying software technology, or scheduled where elements or inputs/outputs are time-based. Scheduled activities are managed through quality control procedures within the operational teams on a daily basis through a catalogue of checklists ensuring prices and other market data are timely and accurate, with any exceptions actioned accordingly. Scheduling and commencement of major batch processes are enacted by authorised personnel, and exceptions in both cases are captured and communicated, and resolved in a timely manner. Scheduled data feed consumption from third party providers are monitored on a daily basis through a purpose built dashboard, with any exceptions followed up in a timely manner.

Safeguarding assets

The safeguarding of assets begins with the design, concepts of classification based isolation and control sets, and is considerate of the data and information lifecycle. Physical safeguarding is controlled and managed by authorised personnel whereby physical access is granted and removed in a timely manner, with exceptions being elevated to building management for immediate deactivation, this is further supported by Praemium CCTV and building management security controls.

Digital assets have appropriate measures and processes in place to identify and reduce the risk of malicious attacks, including information assets, digital infrastructure and data sets, as well as our in-house developed and built software and related components. Access to digital assets, specifically support administrator access (ie: Level 13) to the VMA and SMA platforms, Azure Active Directory which includes Office365, Microsoft Dynamics and other corporate services which require multi factor authentication (MFA).

The logical perimeter is protected by multiple firewall layers with active monitoring and alerting, which includes the termination of secure protocols to allow full content inspection. Antivirus and anti-malware systems exist across the entire estate and are centrally managed again with alerting, with any known incidents investigated promptly and reported in monthly management reports, alongside infrastructure, network and security components. Penetration testing is conducted at least annually by a third party, all outcomes are managed to completion.

Production backups are taken nightly, they are encrypted, verified and regularly restored to a testing environment in a 'cleansed/desensitised' state, ensuring the backup is recoverable and complete. Backup media is routinely moved to a managed secure off-site and off-line storage facility through a managed process by authorised personnel.

Maintaining and developing systems hardware and software

Product Strategy

Product strategy is managed through sessions which are held at least once annually, whereby the CEO, Senior Management, Product Owners and Business Analysts attend working groups to discuss the strategic direction of the business and specifically its products. These discussions focus on high level program and product initiatives which flow into smaller detailed product backlogs which are then managed and groomed regularly by relevant parties and teams.

Application changes

All changes to software follow a consistent, documented and repeatable software development lifecycle. All application changes are deployed using automated release management software, changes are deployed to segregated environments at each stage of the Software Development Lifecycle (SDLC) which is managed by the quality assurance team. Application changes pass through our four environments (Continuous Integration (CI), Test, User Acceptance Testing (UAT) and Production) within our software development lifecycle with manual and automated testing being conducted and defects actioned accordingly. A sign off process is followed to promote the release from the Test environment to UAT, with the final sign off occurring prior to production deployment.

Data migrations

Data migrations are managed by the client, using Praemium's in-house developed data upload functionality tool that carry inbuilt business logic and rules to help them seamlessly manage their data, where additional functionality is required by the client to extend the existing inbuilt business logic and rules migration uploads, such request would be prioritised and developed in accordance with the existing SDLC.

Data modification

Modifications to in-system data are raised through the work management tool to ensure traceability and managed in source repository, with execution managed through automated deployment software where by the change is applied to a 'production like' environment for inspection prior to applying the change to production. Deployment of modifications are segregated by role and deployments managed by authorised individuals. The modifications process is visible to all teams, including those individuals who raised the item, team leaders and some senior management for inspection during the UAT and production phase of the process, this includes the modification scripts and accompanied results as it's applied to the necessary environments.

In the event an unauthorised (intentional or unintentional) or malicious modification is made, there is a process in place that supports a forensic examination of the event, which would result in any modified data being fully reinstated.

Infrastructure

Changes to the production environment, such as modifying the application firewall are handled by senior staff on the Infrastructure team. All requests are raised, discussed for priority/business impact, and approved before being applied. Any changes made are logged and an alert sent to the Infrastructure team with the changelog.

Recovering from processing interruptions

Systems and data are regularly backed up to similarly protected and operated offsite locations and restored regularly as part of our software development lifecycle. IT Disaster Recovery (DRP) and Business Continuity Plans (BCP) are tested at least annually and a Risk Management Plan with a register that complies with Standard AS4360. Results of the disaster recovery tests are available for client consumption and all outcomes are managed to completion. Clients can participate in the coordinated disaster recovery exercise if they so desire.

Hardware and software operational performance and availability is monitored regularly by both automated systems and human operators, and any exceptions that require action are handled and resolved in a timely manner.

Policies, standards and procedures

Praelium has a comprehensive framework of policies which are regularly reviewed. These policies are supported by a number of procedures and checklists.

Monitoring compliance

All clients sign a service agreement with standard terms and conditions, the service agreements do not typically specify service level agreements or performance targets.

Monitoring subservice organisations

External service providers are managed and monitored by the infrastructure team, following rigorous pre-commencement comparison to peers and best of breed international providers of similar services. Access for external providers is intentionally limited or restricted to limit attack surface of any system or environment, with monitoring and auditing occurring where remote access is granted.

Service agreements are in place and any issues, should they arise, are resolved between the Infrastructure team and the service provider.

Subservice Organisations

The Company utilises subservice organisations to perform certain functions to improve the operating and administrative effectiveness. The accompanying description includes only the policies, procedures, and control activities at the Company and does not include the policies, procedures, and control activities at the third-party service organisations described below. The examination by the Independent Service Auditor did not extend to the policies and procedures at these subservice organisations. The most significant subservicing organisations used by the Company are noted below.

Subservice Organisation	Service(s) Provided
MyDBA	Database monitoring
Equinix	Infrastructure hosting and environmental controls
Interactive	Provision of hardware warranties

User Control Considerations

Where controls that are integral to the achievement of the management assertions made by Praemium are operated by Praemium's clients or their Nominated Representatives we have documented these as "complementary user controls" below.

Complementary User Entity Controls	Related Control Objective(s)
The Client's management is responsible for ensuring access to terminals connected to computer systems and located in client facilities are limited to authorised individuals. In addition, clients are responsible for ensuring that appropriate authentication controls are in place and that only authorised and properly trained personnel are given access to systems.	Control Objective G 2
A Client Administrator is created by Praemium for each Service in the Praemium application. The Client Systems Administrator is responsible for the creation and maintenance of application user accounts. The Client Systems Administrator is responsible for setting the password requirements for the Service. The Client Systems Administrator is also responsible for resetting passwords of users within the Service.	Control Objective G 2
The Client is responsible for ensuring that access granted to application users enforces appropriate segregation of duties.	Control Objective G 3
The Client is responsible for ensuring that change requests are raised to Praemium by individuals with appropriate authorisation.	Control Objective G 7
The Client is responsible for ensuring that requests for database updates and modification are appropriately authorised and valid.	Control Objective G 8
The Client is responsible for ensuring the implementation and maintenance of a business recovery plan to support the Client's operations if a critical resource is not available.	Control Objective G 11

4. The Company's Controls and Testing Performed by the Service Auditor

Types and Descriptions of the Tests of Design

Various testing methods are used to assess the design of controls during the Specified Period. The table below describes the various methods which were employed in testing the design of controls that are in place at the Company.

Type	Description
Inquiry	<p>Inquired of appropriate personnel seeking relevant information or representation including, among other things:</p> <p>Knowledge and additional information regarding the policy or procedure; and</p> <p>Corroborating evidence of the policy or procedure.</p> <p>As inquiries were performed for substantially all controls, the test was not listed individually for every control shown in the accompanying matrices.</p>
Observation	<p>Observed the application or existence of specific controls as represented.</p>
Inspection	<p>Inspected documents and records indicating performance of the controls. This testing included, among other things:</p> <ul style="list-style-type: none"> • Inspection of reconciliations and management reports that age or quantify reconciling items to assess whether balances and reconciling items were properly monitored, controlled, and resolved on a timely basis; • Examination of source documentation and authorisations to verify propriety of processed transactions; • Examination of documents or records for evidence of performance, such as the existence of initials or signatures; and <p>Inspection of systems' documentation, such as operations manuals, flow charts, and job descriptions.</p> <p><i>Additionally, where appropriate, inquiries, observation and inspection procedures were performed as it relates to system generated reports and queries in order to assess the accuracy (reliability) of the information used in the execution of control activities.</i></p>
Re-performance	<p>Re-performed the control, or processing of the application control, to help ensure the accuracy of its operation. This testing included, among other things:</p> <ul style="list-style-type: none"> • Obtaining evidence of the arithmetical accuracy and correct processing of transactions by performing independent calculations; and <p>Re-performing the matching of various system records by independently</p>

matching the same records and comparing reconciling items to the Company's prepared reconciliations, if applicable.

Sampling Methodology

Where inspection is the appropriate testing technique, the following annualised sample sizes are indicative of the level of testing performed on each control:

Control frequency	Sample size
Multiple times a day	25
Daily	25
Weekly	5
Monthly	2
Quarterly	2
Annually	1

Automated controls are generally tested once, unless there are relevant weaknesses in IT general controls (ITGCs), in which case additional testing may be performed to assess whether the ITGC weakness has affected the operation of the control.

Control Objectives, Control Activities, Tests Performed and Results of Testing

Section E – Investment Administration

CONTROL OBJECTIVE 1

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

Control Activity		Tests Performed By Service Auditor	Results of Testing
E 1.1	New accounts are created based on an authorised request from the Dealer Group where Praemium are engaged for administration services.	1. Inspection: For a sample of new accounts for Shaw & Partners and Seneca, inspected relevant authorised request form and evidence of account set up in the system to determine that the new account was set up by Praemium based on an authorised request from the Dealer Group.	Effective. No exceptions noted.

CONTROL OBJECTIVE 2

Complete and authorised client agreements are established prior to initiating accounting activity.

	Control Activity	Tests Performed By Service Auditor	Results of Testing
E 2.1	Prior to any activity on accounts commencing, Praemium receives signed application from clients.	1. Inspection: For a sample of new accounts, inspected the application from the client to determine that this was signed and was obtained prior initiating transactions on the account.	Effective. No exceptions noted.

CONTROL OBJECTIVE 3

Portfolio transactions are recorded completely, accurately and on a timely basis.

Control Activity		Tests Performed By Service Auditor	Results of Testing
E 3.1	All broker transactions (buys/sells) for ASX listed entities are updated in the platform via the overnight Broker data feed.	1. Inspection: For a sample of days, inspected evidence of the reconciliations performed between data feeds and the system to determine that these are reviewed independently for accuracy, and any discrepancies between the data feed and system are identified and managed through to resolution.	Effective. No exceptions noted.
		2. Inspection: For a sample non-compulsory corporate actions taken up by an Advisor, determine via walkthrough, whether the Praemium application accurately reflects the acceptance and settlement instructions provided by the Advisor.	Effective. No exceptions noted.
		3. Inspection: For a sample of days, inspected evidence of the reconciliation between the Broker data feed data and Praemium transaction records to determine this was undertaken and issues managed through to resolution.	Effective. No exceptions noted.
E 3.2	All non-broker transactions, with the exception of Term Deposits, are recorded and managed via workflow.	1. Inspection: For a sample of non-broker transactions (excluding term deposit maturity), inspected Zendesk supporting advisor documentation to determine whether the transactions were recorded and managed via workflow.	Effective. No exceptions noted.
E 3.3	Multi-Account Reconciliation (MAR) tool is run on a daily basis to compare holdings from the data feed to the system holdings. All variations are investigated, recorded and followed through to resolution.	1. Inspection: For a sample of days, inspected evidence of the MAR reconciliation to determine these are performed between data feeds and the system to determine these are reviewed independently for accuracy, and any discrepancies between the data feed and system are identified and managed through to resolution.	Effective. No exceptions noted.

CONTROL OBJECTIVE 4

Corporate actions are actioned, processed and recorded accurately and on a timely basis.

	Control Activity	Tests Performed By Service Auditor	Results of Testing
E 4.1	All compulsory corporate action, such as SOA / Mergers / Takeovers/ Reconstructions are monitored and processed by Praemium Corporate Actions (CA) team on a "global" level and processed in the Praemium system on a daily basis.	1. Inspection: For a sample of compulsory corporate actions, inspected evidence of the event managed via the platform and associated tax report to determine whether compulsory corporate actions are monitored and processed by Praemium Corporate Actions team on a "global" level daily.	Effective. No exceptions noted.
E 4.2	All non-compulsory Corporate Actions (CA), are uploaded into the Praemium application via the overnight data feed. Advisors are then responsible for accepting the non-compulsory CA via the Praemium application which is automatically updated on the client account.	1. Walkthrough: Viewed the overseer tool and notification slack channel to determine whether Praemium staff are automatically notified of any errors in the overnight batch recalculation process.	Effective. No exceptions noted.
		2. Inspection: For a sample of days, inspected commencement and completion emails to determine whether the Operations team initiates the overnight processing.	Effective. No exceptions noted.
		3. Inspection: For a sample of days, inspected the Operations Team Corporate Actions Checklist to determine that this has been completed to confirm the overnight process completed successfully.	Effective. No exceptions noted.
		4. Inspection: For a sample non-compulsory Corporate Actions taken up by an Advisor, determine via walkthrough, whether the Praemium application accurately reflects the acceptance and settlement instructions provided by the Advisor.	Effective. No exceptions noted.

CONTROL OBJECTIVE 5

Expenses are appropriately authorised and recorded in accordance with the service level agreement and/or client instructions, on a timely basis.

	Control Activity	Tests Performed By Service Auditor	Results of Testing
E 5.1	Praemium does not authorise expenses. Praemium will record expenses that appear in the client's cash accounts in accordance with client instructions.	1. Inspection: For a sample of expenses, inspected client's account details to determine whether expenses are recorded in the client's cash accounts in accordance with client instructions.	Effective. No exceptions noted.

CONTROL OBJECTIVE 6

Accounts are administered in accordance with client agreements.

	Control Activity	Tests Performed By Service Auditor	Results of Testing
E 6.1	Client requirements as per their agreement are administered via Praemium's workflow system.	1. Inspection: For a sample of new accounts for Shaw & Partners, Seneca and Morgan Stanley, inspected that new accounts set up by VMAAS were based on a signed agreement and completed new account checklist.	Effective. No exceptions noted.
		2. Inspection: For a sample of client requests, determined that these are recorded and managed via the Praemium workflow system.	Effective. No exceptions noted.

CONTROL OBJECTIVE 7

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

	Control Activity	Tests Performed By Service Auditor	Results of Testing
E 7.1	Not applicable to Praemium.		

CONTROL OBJECTIVE 8

Investment income and related tax are accurately calculated and recorded on a timely basis.

	Control Activity	Tests Performed By Service Auditor	Results of Testing
E 8.1	All income relating to "global" assets are maintained by the Corporate Actions team to ensure income is accurately recorded in the Praemium system.	1. Inspection: For a sample of days, inspected the daily checklist to determine that they have been reviewed by a supervisor, with exceptions followed up and resolved in a timely manner.	Effective. No exceptions noted.
E 8.2	Praemium Administration confirms the receipt of expected income and takes action on any income exception items.	1. Inspection: For a sample of income receipts during the period, inspected client cashbook income statements to determine that that the VMAAS team confirms the receipt of expected income and manages exception items to resolution.	Effective. No exceptions noted.
E 8.3	All income relating to "service" assets is manually added on the system by Praemium Administration following client or third party instructions.	1. Inspection: For a sample of receipts of income relating to "service" assets, inspected client cashbook income statements and cash narrations to determine that income is manually added on the system by the VMAAS team following client or third party instructions.	Effective. No exceptions noted.

CONTROL OBJECTIVE 9

Investments are valued using current prices obtained from independent external pricing sources, or an alternative basis in accordance with client agreement.

Control Activity		Tests Performed By Service Auditor	Results of Testing
E 9.1	All ASX/listed prices are updated and processed in the Praemium application via automated data feeds.	1. Inspection: Inspected, via walkthrough, the job schedule configuration for the automation of investment price feed upload to determine that it automatically feeds ASX/listed pricing data directly into the Praemium system.	Effective. No exceptions noted.
		2. Inspection: Inspected, via a walkthrough of one, that the automated price upload is accurately recorded in the Praemium application.	Effective. No exceptions noted.
E 9.2	All non-data fed pricing is provided by the client and managed and recorded via workflow.	1. Inspection: For a sample of non-data fed pricing changes, inspected relevant pricing information, Zendesk ticket and evidence of change in the system to determine that pricing is provided by client and managed and recorded via workflow.	Effective. No exceptions noted.

CONTROL OBJECTIVE 10

Issue and cancellations of shares/units are recorded completely and accurately in the financial records and units on issue are regularly reconciled to data provided by registry.

	Control Activity	Control Activity	Control Activity
E10.1	All compulsory corporate action, such as SOA/Mergers/Takeovers/ Reconstructions are monitored and processed by Praemium Corporate Actions team on a "global" level and processed in the Praemium system on a daily basis. (as per Control E4.1)	1. Inspection: For a sample of compulsory corporate actions, inspected evidence of the event managed via the platform and associated tax report to determine whether compulsory corporate actions are monitored and processed by Praemium Corporate Actions team on a "global" level daily.	Effective. No exceptions noted.
E 10.2	All non-compulsory CAs, are uploaded into the Praemium application via the overnight data feed. Advisors are then responsible for accepting the non-compulsory CA via the Praemium application which is automatically updated on the client account. (as per Control E4.2)	1. Walkthrough: Observed via walkthrough the overseer tool and notification slack channel to determine Praemium staff are automatically notified of any errors in the overnight batch recalculation process.	Effective. No exceptions noted.
		2. Inspection: For a sample of days, inspected commencement and completion emails to determine that the Operations team initiates the overnight processing.	Effective. No exceptions noted.
		3. Inspection: For a sample of days, inspected the Operations Team Corporate Actions Checklist to determine that this has been completed to confirm the overnight process completed successfully.	Effective. No exceptions noted.
		4. Inspection: For a sample non-compulsory CA taken up by an Advisor, determine via walkthrough, whether the Praemium application accurately reflects the acceptance and settlement instructions provided by the Advisor.	Effective. No exceptions noted.

CONTROL OBJECTIVE 10

Issue and cancellations of shares/units are recorded completely and accurately in the financial records and units on issue are regularly reconciled to data provided by registry.

	Control Activity	Control Activity	Control Activity
E 10.3	Multi-Account Reconciliation (MAR) tool is run on a daily basis to compare holdings from the data feed to the system holdings. All variations are investigated, recorded and followed through to resolution. (as per Control E3.3)	1. Inspection: For a sample of days, inspected evidence of the MAR reconciliation to determine these are performed between data feeds and the system to determine these are reviewed independently for accuracy, and any discrepancies between the data feed and system are identified and managed through to resolution.	Effective. No exceptions noted.

CONTROL OBJECTIVE 11

Cash and securities positions are completely and accurately recorded and reconciled to third party data on a timely manner.

Control Activity		Tests Performed By Service Auditor	Results of Testing
E 11.1	Refer to control objective E 3	Refer to control objective E 3	Refer to control objective E 3

CONTROL OBJECTIVE 12

Reconciliations between difference systems, including the investment ledger, general ledger and administration system, are performed on a timely basis.

	Control Activity	Tests Performed By Service Auditor	Results of Testing
E 12.1	Multi-Account Reconciliation (MAR) tool is run on a daily basis to compare holdings from the data feed to the system holdings. All variations are investigated, recorded and followed through to resolution. (as per Control E3.3)	1. Inspection: For a sample of days, inspected evidence of the MAR reconciliation to determine these are performed between data feeds and the system to determine these are reviewed independently for accuracy, and any discrepancies between the data feed and system are identified and managed through to resolution.	Effective. No exceptions noted.

CONTROL OBJECTIVE 13

Errors are identified, notified to clients and rectified promptly in accordance with client agreements.

	Control Activity	Tests Performed By Service Auditor	Results of Testing
E 13.1	A process is in place to identify, record and manage errors or complaints. This includes the investigation of the error, client notification and management through to resolution.	1. Inspection: For a sample of errors, inspected evidence of calculation and remediation activities to determine that errors are recorded, clients are notified and managed through to resolution.	Effective. No exceptions noted.

CONTROL OBJECTIVE 14

Appointments of subservice organisations, including those providing investment administration, are approved, subservice organisations are properly managed, and their activities are adequately monitored on a timely basis.

	Control Activity	Tests Performed By Service Auditor	Results of Testing
E 14.1	Not applicable to Praemium.		

CONTROL OBJECTIVE 15

Periodic reports to clients, including calculation of net asset value if required, are accurate, complete and distributed on a timely basis.

Control Activity		Tests Performed By Service Auditor	Results of Testing
E 15.1	Client data is validated and reconciled on input into the Platform via automated data feeds and reconciliations.	1. Inspection: For a sample of days, inspected the Operations Team Corporate Actions Checklist to determine this has been completed to confirm the overnight process completed successfully.	Effective. No exceptions noted.
		2. 1. Inspection: For a sample of days, inspected evidence of the MAR reconciliation to determine these are performed between data feeds and the system to determine these are reviewed independently for accuracy, and any discrepancies between the data feed and system are identified and managed through to resolution.	Effective. No exceptions noted.
		3. Inspection For a sample of compulsory corporate actions, inspected evidence of the event managed via the platform and associated tax report to determine that compulsory corporate actions are monitored and processed by Praemium Corporate Actions team on a "global" level daily.	Effective. No exceptions noted.
		4. Inspection: For a sample non-compulsory CA taken up by an Advisor, determine via walkthrough, that the Praemium application accurately reflects the acceptance and settlement instructions provided by the Advisor.	Effective. No exceptions noted.
E 15.2	Reports are quality checked and delivered in line with the client agreements.	1. Inspection: For a sample of quarters and a sample of clients, inspected WHAT to determine that reports are quality checked and delivered in line with the client agreements.	Effective. No exceptions noted.

CONTROL OBJECTIVE 16

Annual reports and accounts are prepared in accordance with applicable laws and regulations.

	Control Activity	Tests Performed By Service Auditor	Results of Testing
E 16.1	Refer to control objective E 15	Refer to control objective E 15	Refer to control objective E 15

CONTROL OBJECTIVE 17

Tax Policy is updated and reviewed on a timely basis.

	Control Activity	Tests Performed By Service Auditor	Results of Testing
E 17.1	Corporate Action and Tax policy for corporate actions is documented and reviewed at least annually.	1. Inspection: Inspected the Corporate Action and Tax policy to determine that the Policy was reviewed and updated in the past 12 months.	Effective. No exceptions noted.

CONTROL OBJECTIVE 18

Tax information components and attributes used in the preparation of the income tax computation (current and deferred) are complete and calculated accurately in accordance with tax policy or as agreed with clients.

	Control Activity	Tests Performed By Service Auditor	Results of Testing
E 18.1	Corporate actions are processed as per the Corporate Actions and Tax policy document.	1. Inspection: For a sample of corporate actions, inspected of the event managed via the platform and associated tax report to determine that corporate actions are processed as per the Corporate Actions and Tax policy document.	Effective. No exceptions noted.

CONTROL OBJECTIVE 19

Differences between tax and accounting treatments are identified and calculated in accordance with tax policy or as agreed with clients and reported in a timely manner to clients.

	Control Activity	Tests Performed By Service Auditor	Results of Testing
E19.1	Not applicable to Praemium.		

CONTROL OBJECTIVE 20

Current and deferred tax balances in the general ledger are accurately recorded in accordance with the tax computation and processed in a timely manner in accordance with tax policy or as agreed with clients.

	Control Activity	Tests Performed By Service Auditor	Results of Testing
E20.1	Not applicable to Praemium.		

Section G – Information Technology

CONTROL OBJECTIVE 1

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

Control Activity		Tests Performed By Service Auditor	Results of Testing
G 1.1	Access to the Praemium office is controlled via RFID access cards and is restricted to authorised personnel.	1. Observation: Observed that access to the Praemium office is restricted via the use of RFID cards.	Effective. No exceptions noted.
		2. Inspection: Inspected user access reports to determine that access to the Praemium office is restricted to authorised personnel.	Effective. No exceptions noted.
G1.2	Client data resides in secure data centres managed by third parties.	1. Inspection: Inspected the Agreement in place between Praemium and the third party data centre to determine that a current, signed agreement is in place.	Effective. No exceptions noted.
		2. Inspection: Inspected Data Centre access reports to determine that only authorised individuals have access to the data centre based on their functional role and inquiry with Management.	Effective. No exceptions noted.

CONTROL OBJECTIVE 2

Logical access to computer systems, programs, master 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 Activity		Tests Performed By Service Auditor	Results of Testing
G 2.1	Authentication to the Praemium network requires a valid user ID and password.	1. Inspection: Inspected the Active Directory password configuration and documented Password Policy to determine that the password for the network is configured in line with the password policy.	Effective. No exceptions noted.
		2. Inspection: Inspected the network user access report that each user has a unique user ID assigned for the network.	Effective. No exceptions noted.
G 2.2	Authentication to the Praemium application requires a valid user ID and password.	1. Inspection: Inspected the application Password configuration and documented Password Policy to determine that password for the Praemium application is configured in line with the password policy.	Effective. No exceptions noted.
		2. Inspection: Inspected the Praemium user access report (application) that each user has a unique user ID assigned for the Praemium application.	Effective. No exceptions noted.
G 2.3	Access to client data via the application, database, network and server is granted based on an appropriately approved request.	1. Inspection: For a sample of new users, inspected that their access to each applicable layer (application, database, network and the server) is in line with an appropriately approved request.	Effective. No exceptions noted.
		2. Inspection: For a sample of transferred users, inspected that their access to each applicable layer (application, database, network and the server) is in line with an appropriately approved request.	Effective. No exceptions noted.
G 2.4	Access to Praemium systems is revoked when a user leaves Praemium or no longer requires access for their role.	1. Inspection: For a sample of employees who ceased employment with Praemium, inspected that a 'User termination process checklist' has been completed, signed off by the IT team and access to each applicable layer (application, database, network and the server) has been revoked in a timely manner.	Effective. No exceptions noted.

CONTROL OBJECTIVE 2

Logical access to computer systems, programs, master 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 Activity		Tests Performed By Service Auditor	Results of Testing
G2.5	Administrator access to the application, database, network and server is restricted to users who require this level of access for their role.	1. Inspection: Inspected user access reports to determine that users with administrator access to the application, database, network and server are appropriate based on their functional role and inquiry with Management.	Effective. No exceptions noted.
G2.6	Administrator access to Praemium applications is reviewed on a monthly basis.	1. Inspection: For a sample of months, inspected evidence of the review of administrator access to the Praemium application to determine that this was conducted, and any issues identified were remediated in a timely manner.	Effective. No exceptions noted.
G2.7	Access to the application and network is managed via role-based access.	1. Inspection: Inspected the user access reports for Active Directory to determine that that access to the Praemium network is managed via role-based access.	Effective. No exceptions noted.
		2. Inspection: Inspected the user access reports for the Praemium application to determine that that access to the Praemium application is managed via role-based access.	Effective. No exceptions noted.
G 2.8	Only authorised users have access to modify client data.	1. Inspection: Inspected user access reports to determine that only authorised users are able to modify client data via the Database Update (DBU) process.	Effective. No exceptions noted.
G 2.9	Access to the Praemium network and application are restricted via the use of two factor authentication.	1. Observation: Observed, via walkthrough, that remote access is restricted via the use of two factor authentication.	Effective. No exceptions noted.

CONTROL OBJECTIVE 3

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

Control Activity		Tests Performed By Service Auditor	Results of Testing
G3.1	Access to the application and network is managed via role-based access. (as per Control 2.7)	1. Inspection: Inspected the user access reports for Active Directory to determine that that access to the Praemium network is managed via role-based access.	Effective. No exceptions noted.
		2. Inspection: Inspected the user access reports for the Praemium application to determine that that access to the Praemium application is managed via role-based access.	Effective. No exceptions noted.
G 3.2	The development and production environments are segregated.	1. Inspection: Inspected that the development and production environments to determine that these are logically segregated.	Effective. No exceptions noted.
G 3.3	Only authorised application administrators hold access to the development environment.	1. Inspection: Inspected user access reports to determine that only authorised application administrators have access to the development environment based on their functional role and inquiry with Management.	Effective. No exceptions noted.
G 3.4	Users with Network Administrator access do not have Praemium Application Administrator access.	1. Inspection: Inspected user access reports to determine that network administrators and Praemium application administrators are segregated.	Effective. No exceptions noted.
G 3.5	All changes to the Praemium application require testing to be performed and changes authorised prior to implementation.	1. Inspection: For a sample of changes, inspected change records to determine that User Acceptance Testing (UAT) was completed.	Effective. No exceptions noted.
		2. Inspection: For a sample of changes, inspected change records to determine that approval from Quality Assurance (QA) was gained prior to release into production.	Effective. No exceptions noted.

CONTROL OBJECTIVE 3

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

Control Activity		Tests Performed By Service Auditor	Results of Testing
G3.6	Logical access to develop and implement changes is segregated, with the exception of users who require access for support and oversight purposes.	1. Inspection: Inspected user access reports to determine that users responsible for application development do not have access to deploy changes with the exception of users who require access for support and oversight purposes. Determine that users with access to both develop and implement changes is necessary based on their functional role and inquiry with Management.	Effective. No exceptions noted.
G 3.7	Logical access controls have been established to ensure appropriate segregation between staff responsible for the preparation and execution of modifications to client data.	1. Inspection: Inspected that segregation of duties controls have been established via logical access controls for the preparation and release of modification to client data. Determine that users with access to both the preparation and release is necessary based on their functional role and inquiry with Management.	Effective. No exceptions noted.
G 3.8	Only authorised users are able to modify the Praemium application source code.	1. Inspection: Inspected user access reports to determine that access to modify Application source code is appropriately restricted to users who require this access for their functional role based on inquiry with Management.	Effective. No exceptions noted.

CONTROL OBJECTIVE 4

IT processing is authorised and scheduled appropriately and exceptions are identified and resolved in a timely manner.

Control Activity		Tests Performed By Service Auditor	Results of Testing
G 4.1	IT processing jobs are manually initiated, and management of these jobs is restricted to authorised individuals.	1. Inspection: Inspected user access reports to determine that access to initiate and alter batch processing jobs is restricted to authorised personnel based on their functional role and inquiry with Management.	Effective. No exceptions noted.
G 4.2	Overnight processing jobs are monitored and exceptions followed up in a timely manner.	1. Observation: Observed via walkthrough the overseer tool and slack channel used for notifications, to determine that Praemium staff are automatically notified of any errors in the overnight batch recalculation process.	Effective. No exceptions noted.
		2. Inspection: For a sample of days, inspected commencement and completion emails to determine that the Operations team initiates the overnight processing.	Effective. No exceptions noted.
		3. Inspection: For a sample of days, inspected the Corporate Actions Checklist prepared by the Operations Team, to determine this has been completed to confirm the overnight process completed successfully.	Effective. No exceptions noted.
G4.3	The Corporate Actions Team verify the batch process was completed on the following business day.	1. Inspection: For a sample of days, inspected the daily checklist to determine that this has been reviewed by a supervisor, and exceptions were followed up and resolved in a timely manner.	Effective. No exceptions noted.
G4.4	End of Day Pricing Feeds are reviewed daily and exceptions followed up in a timely manner.	1. Inspection: For a sample of days, inspected the daily checklist to determine that the end of day pricing feed was reviewed and exceptions were followed up and resolved in a timely manner.	Effective. No exceptions noted.

CONTROL OBJECTIVE 5

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

Control Activity		Tests Performed By Service Auditor	Results of Testing
G 5.1	All servers and workstations are protected by anti-virus and anti-malware software.	1. Inspection: Inspected the CrowdStrike Dashboard to determine that servers and workstations are protected by anti-virus and anti-malware software.	Effective. No exceptions noted.
G5.2	Penetration testing is undertaken annually by a third party. The scope of the annual penetration test excludes Powerwrap systems in maintenance only mode.	1. Inspection: Determine that penetration tests are conducted at least annually.	Effective. No exceptions noted.
		2. Inspection: Determine that the penetration test report was reviewed by Praemium staff and action items were assigned and subsequently tracked to remediation.	Effective. No exceptions noted.
G5.3	Firewalls are in place to protect the network and key applications from malicious attacks.	1. Inspection: Inspected the network diagram and current firewall versions to determine that firewalls have been implemented within the network.	Effective. No exceptions noted.
G 5.4	Changes to firewall parameters are conducted in accordance with Praemium Firewall Change Procedure.	1. Inspection: Inspected the user access report to determine that only authorised individuals have access to make changes to the firewall based on their functional role and inquiry with Management.	Effective. No exceptions noted.
		2. Inspection: For a sample of changes to firewall parameters, inspected change records to determine that that they were completed in accordance with Praemium Firewall Change Procedure.	Effective. No exceptions noted.
G 5.5	All changes are subject to vulnerability scanning as part of the development cycle prior to release to production.	1. Inspection: Inspected via walkthrough that SonarCloud has been configured to perform vulnerability scanning over all changes prior to release to production.	Effective. No exceptions noted.

CONTROL OBJECTIVE 6

Client data is appropriately stored to ensure security and protection from unauthorised use.

	Control Activity	Tests Performed By Service Auditor	Results of Testing
G 6.1	Client data resides in secure data centres managed by third parties. (as per Control G1.2)	1. Inspection: Inspected the Agreement in place between Praemium and the third party data centre to determine that a current, signed agreement is in place.	Effective. No exceptions noted.
		2. Inspection: Inspected Data Centre access reports to determine that only authorised individuals have access to the data centre based on their functional role and inquiry with Management.	Effective. No exceptions noted.
G 6.2	Client data backups are encrypted prior to being stored off-site.	1. Inspection: Inspected the configuration of backup jobs to determine that backups are configured to encrypt data during the backup process.	Effective. No exceptions noted.
G 6.3	Access to the Praemium office is controlled via RFID access cards and is restricted to authorised personnel. (as per Control G1.1)	1. Observation: Observed that access to the Praemium office is restricted via the use of RFID cards.	Effective. No exceptions noted.
		2. Inspection: Inspected that access to the Praemium office is restricted to authorised personnel.	Effective. No exceptions noted.
G 6.4	Access to client data via the application, database, network and server is granted based on an appropriately approved request. (as per Control G2.3)	1. Inspection: For a sample of new users, inspected that their access to each applicable layer (application, database, network and the server) is in line with an appropriately approved request.	Effective. No exceptions noted.
		2. Inspection: For a sample of transferred users, inspected that their access to each applicable layer (application, database, network and the server) is in line with an appropriately approved request.	Effective. No exceptions noted.

CONTROL OBJECTIVE 6

Client data is appropriately stored to ensure security and protection from unauthorised use.

	Control Activity	Tests Performed By Service Auditor	Results of Testing
G 6.5	Access to the application and network is managed via role based access. (as per Control G2.7)	1. Inspection: Inspected the user access reports for Active Directory to determine that that access to the Praemium network is managed via role based access.	Effective. No exceptions noted.
		2. Inspection: Inspected the user access reports for the Praemium application to determine that that access to the Praemium application is managed via role based access.	Effective. No exceptions noted.
G 6.6	Administrator access to the application, database, network and server is restricted to users who require this level of access for their role. (as per Control G2.5)	1. Inspection: Inspected user access reports to determine that users with administrator access to the application, database, network and server are appropriate based on their functional role and inquiry with Management.	Effective. No exceptions noted.
G 6.7	Administrator access to Praemium applications is reviewed on a monthly basis. (as per Control G2.6)	1. Inspection: For a sample of months, inspected evidence of the review of administrator access to the Praemium application to determine that this was conducted, and any issues identified were remediated in a timely manner.	Effective. No exceptions noted.
G 6.8	Firewalls are in place to protect the network and key applications from malicious attacks. (as per Control G5.3)	1. Inspection: Inspected the network diagram and current firewall versions to determine that firewalls have been implemented within the network to counter the threat of malicious electronic attack.	Effective. No exceptions noted.
G 6.9	Penetration testing is undertaken annually by a third party. The scope of the annual penetration test excludes Powerwrap systems in maintenance only mode. (as per Control G5.2)	1. Inspection: Determine that penetration tests are conducted at least annually.	Effective. No exceptions noted.
		2. Inspection: Determine that the penetration test report was reviewed by Praemium staff and action items were assigned and subsequently tracked to remediation.	Effective. No exceptions noted.

CONTROL OBJECTIVE 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 Activity		Tests Performed By Service Auditor	Results of Testing
G 7.1	Changes to the Praemium application are logged and managed via the change management system in line with procedures.	1. Inspection: Inspected the Change Management Procedure to determine that this is in place and reviewed annually.	Effective. No exceptions noted.
		2. Inspection: Inspected change records to determine that changes are tracked within a change management software tool.	Effective. No exceptions noted.
G 7.2	All changes to the Praemium application require testing to be performed and changes authorised prior to implementation. (as per Control 3.5)	1. Inspection: For a sample of changes, inspected change records to determine that User Acceptance Testing (UAT) was completed.	Effective. No exceptions noted.
		2. Inspection: For a sample of changes, inspected change records to determine that approval from Quality Assurance (QA) was gained prior to release into production.	Effective. No exceptions noted.
G 7.3	All changes are subject to vulnerability scanning as part of the development cycle prior to release to production. (as per Control G5.5)	1. Inspection: Inspected via walkthrough that SonarCloud has been configured to perform vulnerability scanning over all changes prior to release to production.	Effective. No exceptions noted.

CONTROL OBJECTIVE 8

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

Control Activity		Tests Performed By Service Auditor	Results of Testing
G 8.1	Migration of data follows a controlled process requiring authorisation, testing and reconciliation.	1. Inspection: Inspected the DevOp Procedure to determine that this has been defined and reviewed annually for data migration activity.	Effective. No exceptions noted.
G 8.2	Migration of data are authorised by appropriate personnel prior to migration.	1. Inspection: For a sample of data migrations, inspected that this has been approved prior to migration.	N/A – there were no occurrences of this control in operation during the period as no data migration activity occurred during the period.
G 8.3	Migration of data is tested prior to migration.	1. Inspection: For a sample of data migrations, inspected that testing was completed prior to migration.	N/A – there were no occurrences of this control in operation during the period as no data migration activity occurred during the period.
G 8.4	Data is reconciled once migrated.	1. Inspection: For a sample of data migrations, inspected that a reconciliation of data was completed post migration.	N/A – there were no occurrences of this control in operation during the period as no data migration activity occurred during the period.
G8.5	Modification of client data follows a controlled process requiring authorisation, testing and reconciliation.	1. Inspection: Inspected that the Data Modification Procedure has been defined and reviewed during the period.	Effective. No exceptions noted.
G8.6	All modifications to client data are documented and tracked within a change management system.	1. Inspection: Inspected change records to determine that modification of changes were logged, documented and tracked within the change management system.	Effective. No exceptions noted.
G8.7	Modification to client data must be authorised by appropriate personnel prior to implementation.	1. Inspection: For a sample of direct data changes, inspected change records to determine that the package of modifications to client data were approved by authorised personnel prior to implementation.	Effective. No exceptions noted.

CONTROL OBJECTIVE 8

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

Control Activity		Tests Performed By Service Auditor	Results of Testing
G8.8	Changes to client data (including bank account and user information) are logged and retained.	1. Inspection: Inspected change records to determine that changes to client data are logged and retained.	Effective. No exceptions noted.
G8.9	Automated notifications are configured to communicate modifications to client data to the development team at the time of change.	1. Observation: Observed via walkthrough that automated notifications are configured to notify the IT team of modifications to client data at the time of change.	Effective. No exceptions noted.
G8.10	Only authorised users have access to modify client data. (as per Control 2.8)	1. Inspection: Inspected user access reports to determine that only authorised users are able to modify client data via the Database Update (DBU) process.	Effective. No exceptions noted.

CONTROL OBJECTIVE 9

Data and systems are backed up regularly, retained offsite and regularly tested for recoverability.

Control Activity		Tests Performed By Service Auditor	Results of Testing
G 9.1	Backup jobs are automatically scheduled to backup client data and systems.	1. Inspection: Inspected the Backup Procedure to determine this is in place and reflects the current process.	Effective. No exceptions noted.
		2. Inspection: Inspected the backup schedule to determine that this is configured for source code, production and other key servers.	Effective. No exceptions noted.
G 9.2	Backup jobs are monitored and exceptions followed up in a timely manner.	1. Inspection: For a sample of days, inspected the Backup Status Reports to determine that backups successfully completed, and any errors are followed up in a timely manner.	Effective. No exceptions noted.
G 9.3	Overnight backups are taken to an off-site location.	1. Observation: Observed that backup tapes/media are maintained in an off-site storage facility.	Effective. No exceptions noted.
		2. Inspection: Inspected that a log of backup tapes/media is maintained.	Effective. No exceptions noted.
G 9.4	Restorations of data backups are performed on a regular basis.	1. Inspection: Inspected restoration configuration to determine that that data backups are restored on a regular basis.	Effective. No exceptions noted.
G 9.5	The system is replicated regularly to the Disaster Recovery site.	1. Inspection: Inspected replication configuration to determine that the system is configured to replicate to a Disaster Recovery site.	Effective. No exceptions noted.

CONTROL OBJECTIVE 10

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

Control Activity		Tests Performed By Service Auditor	Results of Testing
G 10.1	The production environment is monitored by automated monitoring tools.	1. Inspection: Inspected 'GOD' tool configuration to determine that production monitoring tools are installed and automatic alerts are enabled.	Effective. No exceptions noted.
		2. Inspection: Inspected the Agreement in place with a third party to determine that third-party monitoring of the production environment is in place and critical faults are raised with the Infrastructure team.	Effective. No exceptions noted.
G 10.2	IT hardware and software issues are recorded and managed via a resolution process.	1. Inspection: Inspected the Agreement in place with a third party provider to determine they are engaged to manage IT hardware and software issues following the end of warranty.	Effective. No exceptions noted.
		2. Inspection: Inspected a sample Fresh Service tickets to determine that software issues follow Praemium's change management procedure.	Effective. No exceptions noted.

CONTROL OBJECTIVE 11

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

Control Activity		Tests Performed By Service Auditor	Results of Testing
G 11.1	An approved Business Continuity Plan is in place for Praemium which reflects the current business environment.	1. Inspection: Inspected that a Business Continuity Plan (i.e. Redbook) has been established, and is reviewed and approved annually.	Exception Noted Whilst testing of the Business Continuity Plan (BCP) took place, the documentation (i.e. Redbook) was not reviewed and approved during the audit period.
G 11.2	The Business Continuity Plan is tested annually via a table-top exercise.	1. Inspection: Inspected that the Business Continuity Plan is tested annually via a table-top exercise.	Effective. No exceptions noted.
G 11.3	An approved Disaster Recovery Plan is in place for the Praemium application which reflects the current environment.	1. Inspection: Inspected that the Disaster Recovery Plan has been established and is reviewed and approved annually.	Effective. No exceptions noted.
G 11.4	The Disaster Recovery Plan is tested annually.	1. Inspection: Inspected that the Disaster Recovery Plan is tested annually.	Effective. No exceptions noted.

CONTROL OBJECTIVE 12

VMA clients sign a Standard Agreement with standard Terms and Conditions, which do not stipulate service levels or targets. Services are delivered to clients in accordance with the Agreement.

Control Activity		Tests Performed By Service Auditor	Results of Testing
G 12.1	A signed agreement is in place for all services provided to clients.	1. Inspection: For a sample of new clients during the period, inspected that a signed agreement was in place.	Effective. No exceptions noted.

CONTROL OBJECTIVE 13

Outsourced activities are approved and managed in accordance with the requirements of the client agreement.

Control Activity		Tests Performed By Service Auditor	Results of Testing
G 13.1	A signed agreement is in place for all third party organisations.	1. Inspection: For all outsourced providers, inspected that a current signed agreement is in place.	Effective. No exceptions noted.
G 13.2	Performance of providers is managed through exception reporting.	1. Inspection: For a sample of months, inspected the monthly Infrastructure Report to determine that third party performance is assessed and reported.	Effective. No exceptions noted.

CONTROL OBJECTIVE 14

Modification of data is documented, authorised, logged, and reviewed.

Control Activity		Tests Performed By Service Auditor	Results of Testing
G 14.1	The Corporate Actions Team verify the batch process was completed on the following business day. (as per Control E4.2)	1. Inspection: For a sample of days, inspected the daily checklist to determine that they have been reviewed by a supervisor, and exceptions were followed up and resolved in a timely manner.	Effective. No exceptions noted.
G 14.2	End of Day Pricing Feeds are reviewed daily and exceptions followed up in a timely manner. (as per Control E4.4)	1. Inspection: For a sample of days, inspected the daily checklist to determine that the end of day pricing feed was reviewed and exceptions were followed up and resolved in a timely manner.	Effective. No exceptions noted.
G14.3	Overnight processing jobs are monitored and exceptions followed up in a timely manner. (as per Control E4.2)	1. Inspection: Inspected via walkthrough the overseer tool slack channel used for notifications, to determine that Praemium staff are automatically notified of any errors in the overnight batch recalculation process.	Effective. No exceptions noted.
		2. Inspection: For a sample of days, inspected the commencement and completion emails to determine that the Operations team initiates the overnight processing.	Effective. No exceptions noted.
		3. Inspection: For a sample of days, inspected the Operations Team Corporate Actions Checklist to determine this has been completed to confirm the overnight process completed successfully.	Effective. No exceptions noted.

5. Other information not covered by the Auditor's report

The information in this section describing activities and controls is presented by Praemium to provide additional information to its users and is not part of the Auditor's report. Such information has not been subjected to the procedures applied in the examination of the description of the Company's operations on behalf of its users, and accordingly, the Service Auditor did not express an opinion on it.

CONTROL OBJECTIVE 11

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

Control Activity		Tests Performed By Service Auditor	Results of Testing
G 11.1	An approved Business Continuity Plan is in place for Praemium which reflects the current business environment.	1. Inspection: Inspected that a Business Continuity Plan (i.e. Redbook) has been established, and is reviewed and approved annually.	Whilst testing of the Business Continuity Plan (BCP) took place, the documentation (i.e. Redbook) was not reviewed and approved during the audit period.

Management's Response: Management accepts the finding as presented. Immediate changes to update the plans have been initiated with a project being scoped to address all uplift requirements.

A new role has been developed in the Risk and Governance Team – Head of Risk Integration – who has the responsibility of the Business Continuity Plans and Policies for the entity moving forward.

Owner: Beth Hyatt, Head of Risk Integration

Target Date: 31 December 2023