AIST Investment Manager Operational Due Diligence Guidance Note
July 2022

Introduction

The Australian Prudential Regulatory Authority ('**APRA**') regularly communicates its expectations with the entities that it regulates, and in 2014 via a publication aimed at Registrable Superannuation Entities ('**RSEs'**) called *Insight*, did so in relation to operational due diligence ('**ODD**') on investment managers. Since then, APRA has regularly made its expectations clear, drawing RSEs' attention to the need for, and importance of, ODD. APRA now routinely assesses RSE processes for managing both investment and operational risk when appointing investment managers/investing in external products.

ODD is defined as "the process of analysing the philosophy, people and processes of the investment manager to ensure that it is able to perform the functions for which it has been appointed".[1]

ODD reviews are essential for the RSE licensee to understand the ability of the investment manager/product to adequately deliver on its representations, and hence be able to fulfil its intended role in meeting the RSE licensee's investment strategy and achieving its investment objectives. As well as the *Insight* article, this is reinforced by the requirements of Prudential Standard SPS 530 Investment Governance ('SPS 530') and Prudential Standard SPS 231 Outsourcing ('SPS 231'). Furthermore, Prudential Standard SPS 220 Risk Management ('SPS 220') emphasises the obligation to have an appropriate risk management framework addressing all material risks.

The ODD review should be viewed as a process to identify and rate the operational risks of engaging an investment manager and is one component that form part of the overall evaluation of an investment manager. The risks identified through the ODD assessment may, on their own, be too significant for an RSE's risk appetite and may in some cases result in a decision to not appoint or continue with an investment manager. Equally, an RSE may note the risks identified during the ODD assessment and may request the investment manager to address and mitigate the risks identified or seek to apply additional controls independent of the investment manager to mitigate to an acceptable level. Both approaches are valid, and it is ultimately each individual RSE's responsibility to determine the acceptable level of risks.

This Guidance Note ('GN') provides guidelines that can be applied to pooled vehicles and Investment Management Agreements ('IMAs') and covers all asset classes, both listed and unlisted.

The examples of good practice and poor practice are included to assist ODD professionals and fund managers in applying consistent evaluations across the industry. It is recognized that some examples may not suit a particular RSE's risk appetite and the examples are not intended to be a checklist of requirements. The examples have been developed through broad and thorough consultation.

The GN operates alongside and is subject to existing laws and regulations. Where there is any conflict or inconsistency between the GN and any law or regulation, that law or regulation prevails.

[1] APRA Insight No.1 2014

Investment Manager Operational Due Diligence Review Process

The Australian Institute of Superannuation Trustees ('AIST'), via a dedicated Working Group of RSE representatives, has developed this GN as a key way of facilitating the ODD review process. Investment managers supplying services to RSEs are encouraged to participate in this process to assist an existing or prospective client with meeting its regulatory requirements.

The ODD review process must be conducted by an appropriately qualified and experienced professional that is independent of the investment manager/product and has the appropriate skills to provide a meaningful, qualitative and quantitative report (ODD Provider). AIST is not able to recommend any such firms other than to note that APRA expects that any RSE relying on the ODD conducted will need to be satisfied of the skill and independence of the professionals conducting the ODD.

It is expected that any potential conflicts of interest are disclosed by a third party conducting an ODD review. This disclosure should include other existing relationships between the third party and the investment manager subject to the review.

APRA has been clear in its communication with the RSEs that appropriate attention must be given to operational risk policies and processes but also to the risk culture within an investment management organization. That is, this is not a "tick the box" exercise and it is expected that the ODD Provider expresses an independent view of the investment manager's policies and practices. AIST expects that the ODD review process may include a mix of desktop policy reviews, questionnaires and detailed on-site due diligence. Guidance is provided within each section that sets a minimum level of ODD considered to be appropriate. However, AIST notes that each RSE and ODD Provider will have their own processes and procedures. Consequently, it is understood that there may be a requirement to apply "enhanced" reviews for additional inquiry depending on the specific investment manager/product.

It is expected that the ODD review be of an advisory nature, and require qualitative, including a relative and comparative appraisal of an investment manager's operations vs peers and good practice.

AIST observes that an ODD report is not a proxy, or replacement, for a GS007 report or any such other "audit" report, nor is a GS007 report an alternative to an ODD review. These reports are complementary and link an organisation's past practices and processes to a forward-looking assessment of its ability to fulfil its operational, legal, and regulatory responsibilities.

Good practice is for the responsibility of the ODD review to be overseen by an experienced, independent person within the RSE who is not aligned to the selection and management of the investment manager, i. e. to ensure an objective assessment can be made that is independent from the investment decision.

AIST notes that the receipt of an ODD report does not exonerate the Trustee of the obligation and responsibility of ensuring that operational risk is identified, assessed, and managed within the risk management framework of the RSE; the ODD report is part of the information used by the Trustee to make its operational risk assessment.

Outcome of the Investment Manager Operational Due Diligence Review Process

Investment managers choosing to support their current and prospective RSE clients can assist by asking providers of ODD services to use this GN as the basis for review. This will create a consistent, hence cost effective, streamlined process which will help the RSE licensees assess operational and associated risks when deciding on the appointment of an investment manager.

AIST's preferred outcome of the ODD review process is for the ODD Provider to prepare an ODD report (the "Report") which outlines any Operational Risk(s) to be considered when deciding to appoint an investment manager. AIST acknowledges that there may be variation in the Report which will depend on the ODD Provider chosen to conduct the ODD review. The Report will be provided to the investment manager by the ODD Provider, and, similar to the process for a GS007 report for example, the investment manager will make the Report available to existing and prospective clients on request.

Under AIST's framework, a full ODD review should be conducted at least every three years, complemented by regular updates from the investment manager on their operations, personnel, governance, risk management and compliance processes. If a material event is notified that is outside the RSE Board's risk appetite for investment governance risk, then this could trigger an earlier review of the investment manager's operations. Examples of a material event could be a valuation/unit pricing adjustment or error, core system/process change/s, security/cyber event, or key personnel changes.

General Requirements in this Guidance Note

The ODD review process needs to take into consideration the criteria detailed in the following eleven key principles:

- Organisational Structure;
- Personnel;
- Governance (including risk management, compliance, related party issues and the corporate social responsibility approach of the firm);
- Trading Processes and Operational Functions (including the ability to identify individual assets, settlement and confirmations, trade allocation processes, trade error identification and handling errors, pre-trade compliance, reconciliations, segregation of duties and registration of assets);
- Valuations;
- IT Systems and Security (including cyber security and security controls);
- Business Continuity and Disaster Recovery;
- Service Provider Oversight;
- Reporting (including reporting on investment related matters);
- Environmental, Social and Corporate Governance; and

- Data Governance & Management.

These principles may change in time as updated practices and requirements emerge. The process to develop the Report will require consideration of each of the above areas.

The May 2022 iteration of the GN has been supplemented by Indicators of Good Practice and Indicators of Poor Practice to provide further assistance to RSEs. In relation to the governance criteria, some of the detailed indicators can be applied by the RSE in a way that recognises the size and resources of smaller investment managers.

AIST has developed this approach to streamline the ODD review process. However, any RSE reserves the right to undertake their own ODD of investment managers and the provision of a Summary Report to an existing or prospective client will not necessarily preclude this from happening.

Ultimately RSEs wish to manage their operational risk prudently whilst doing so in the most economic and efficient manner.

The AIST Working Group/AIST will review this GN on an annual basis to ensure that it remains relevant and will update it for any changes to APRA requirements that may emerge.

AIST Investment Operations Special Interest Group

Contact: David Haynes, Senior Policy Manager, AIST

dhaynes@aist.asn.au

1. Organisational Structure

Objective: To review and assess the organisation's structure and whether any risks have been identified leading to concern that the structure cannot support the investment management process. Specifically focus existence of a robust risk culture across the investment manager's entire organisation.

Issues to be considered.

Review of Policies and Other Written Materials

- Ownership and legal structure (including any subsidiaries and their relation to the investment manager), business strategy (including any future business developments), office locations and affiliated businesses, including the ultimate Owner of the investment manager.

- Board structure and composition including committee membership, skill, roles, independence, role statements and responsibilities in accordance with the principles outlined by the ASX Corporate Governance Council having regard to the nature and scale of the investment manager's operations and any oversight from its parent company (where applicable).

- Policies and documentation in respect of the overall operating model including an overview of the entity, statement of key processes followed, process for regular review including any interactions with outsourcing service providers. *(Note that more detail is specifically requested on a number of these areas later in the GN.)*

- Reference to the total funds under management by asset class, and any overall capacity issues, including client numbers, concentration and risks relevant to the business.

- A copy of an Australian Financial Services License confirming it is a regulated financial services institution in Australia or, if not in Australia, the equivalent documentation for its jurisdiction.

- Review audited financial statements.

- Confirmation in writing that the investment manager has professional indemnity, electronic and computer crime insurance coverage with copies of certificates of currency provided. The level of insurance cover and any key exclusions or non-standard terms should be noted.

Qualitative Assessment and Observations

- Ensure the ownership and legal structure is reasonable for the entity's business model. Ensure the business provides the level of operational support needed to implement its investment strategies. Identify any issues in the business that may lead to a weakness in the ability of the organisation to provide appropriate operational support to the investment decision making.

- Assess the governance model implied in the Board and Committee structures. Assess if it is good practice and, if not, where are the deficiencies. Check for evidence of strong governance and decision making which enables appropriate operational support for investment management.

- The investment manager must be financially sound and stable and ideally provide at least the last three years audited financial statements for review. If appropriate, request a Letter of Comfort from

the manager's auditor regarding the financial stability of the entity or provision of the audit management letter.

- Check the strength of the delegation framework, the risk culture, and its level of permeation through the business, including support from senior management.

- The legal and tax structure of the investment vehicle (i. e., pooled vehicles) where appropriate. This is particularly important for complex, offshore vehicles with layered or feeder structures.

- The level of transparency exhibited by the investment manager when responding to ODD questions during this review (noting, this is difficult to measure, however, important in the assessment of risk culture).

Indicators of Good Practice

- A clear organisational structure diagram is maintained and provided.
- Boards and Board Committees include independent Directors with a diverse range of background and skillset. If Boards or Board Committees do not include independent Directors, good practice is to have an independent Board Advisory Committee supporting the Board.
- Boards, Board Committees and Management Committees are governed by formal Charters and hold regular meetings, which have minutes.
- Clear reporting structure from Management to Boards and Board Committees, ensuring clear segregation and independence based on the 3-lines of defence model.

Indicators of Poor Practice

- Ownership/legal structure appears too complex or opaque.
- Unclear reporting lines and governance structures, or informal governance structures.
- Lack of oversight mechanisms for outsourced service providers.
- Background check on company's ultimate beneficial owner reveals that the beneficial owner is a Politically Exposed Person ("PEP"), criminal or banned from trading.
- Adverse media monitoring reports relating to the investment manager and any Key Persons.
- Undue influence by corporate owner which could result in conflicts of interest.
- Lack of independence and diversity for Board and its committees.
- There is a history of material regulatory breaches. Firm/key personnel has been subject to criminal investigation, lawsuits or convicted of a crime due to fraudulent or dishonest behaviours.
- Inadequate insurance coverage or history of claims indicating operational deficiencies or other factors that could compromise performance.
- Unexplained significant decrease in assets under management which may suggest financial instability or ongoing concern issues.
- Inability to share policies or frameworks, citing "Intellectual Property" concerns for multiple areas requested.

2. Personnel

Objective: To assess in its entirety the investment manager's personnel policies and be assured that it is able to attract, train and retain staff consistent with the culture and philosophy of the organisation.

Issues to be considered.

Review of Policies and Other Written Materials

- Company Code of Conduct (or other standard on ethical/professional behaviour) and all related policies. Biographies of all key personnel, ensuring that an attestation of background checks is available. Relevant experience and roles for all key staff in the investment (to the extent they are responsible for operational work or outcomes) and operational teams. Specific reference should be made to compliance to regulatory requirements such as RG146. Ensure that risk, governance, and compliance staff are included in such checks.

- Written remuneration, staff training and retention/succession planning policies. Does the policy include practices to ensure equivalent pay for equivalent performance and experience regardless of gender and minority group categorisation?

- Team management policies and processes to always ensure appropriate staff coverage.

- Review responsibility of each key staff member and performance reviews in conjunction with the remuneration policy and personal trading policy.

- Team statistics such as size, future hiring plans, turnover, and reasons for turnover.

- Formal Diversity and Inclusion policy or initiative, with procedures and practices in place to ensure that there is an inclusive working environment for all employees.

- Flexible working arrangement available for employees including family and parental leave.

Qualitative Assessment and Observations

- An assessment of the processes to ensure staff are continually confirming compliance with the Company Code of Conduct, or equivalent document and an opinion on appropriate evidence supporting such practice.

- An assessment of the capability and numbers of key staff in the operational area.

- An identification of key person risk and the strategy in place to mitigate the risk.

- A review of how operational staff are recruited and the extent to which background checks and testing capability occurs.

- Review the personal trading policy and test the appropriateness for the nature of the relevant mandate; and, that it is being monitored by appropriately independent persons.

- Review the roles and capability of staff in relation to compliance, risk, and governance. Aspects to consider include the number of roles held, the capacity for genuine segregation of duties and for independent monitoring of the various trading and operational aspects of the business.

- Review and assess policies on Diversity and Inclusion and consider the implementation of such policies. Including how does senior leadership advocate for diversity and inclusion initiatives within the investment management business and/or investment industry. Any defined goals for creating more diverse and inclusive teams at the senior level.

- Review and assess policies on harassment, discrimination, bullying and/or workplace violence in and/or outside of the workplace.

- Check documented procedures are in place for the anonymous reporting, investigation and management of harassment, discrimination, bullying and/or workplace violence. This includes checking whether policies and the procedures are in place to encourage and protect the "whistle blower".

The Report should review the capability of all relevant staff, the number of staff involved in various functions, the level of responsibility held and the quality of and adherence to the policies that support the personnel.

Indicators of Good Practice

- Formal annual or semi-annual performance reviews conducted by line managers with reference to set Key performance indicators ('KPI's') that comprise of a mix of qualitative and quantitative elements. KPI's may include contributions towards achieving the company's ESG target and risk culture.
- Reasonable vesting periods for long term incentives.
- Documented formal succession plan for key senior executives.
- Additional development and learning opportunities available to staff to upskill, for example opportunities to attend conferences and pursue higher education, i.e., CFA program.
- If flexible working arrangements for staff are offered, then it is good practice to have these formalised.
- Formal Diversity and Inclusion policy, with programs and practices embedded within the organisation, with accountability for Diversity and Inclusion.
- A formal whistle-blowing policy, with an external whistle blowing hotline and regular reporting to the board.
- Annual attestation to all employees confirming compliance with Code of Conduct.

Indicators of Poor Practice

- Lack of appropriately qualified and experienced personnel in critical positions. Over-reliance on small number of individuals. No formal succession plan in place.
- Significantly higher staff turnover compared to industry peers across multiple functions.
- Lack of segregation of duties between investment, operations, risk and compliance/control functions.
- Staff remuneration is not formalised or too short-term focused. Remuneration practices are not aligned with the clients' best interests.

- No formal staff appraisal process in place. Staff do not have defined goals or objectives or KPIs'. KPIs do not consider qualitative criteria, e.g., adherence to the Code of Conduct/Ethics or risk management requirements.
- Lack of or insufficient staff training and development, particularly for regulatory and compliance requirements.
- Insufficient evidence of a clear process or procedures for employee disclosure, and the subsequent management and resolution of harassment and misconduct claims.
- Background checks not conducted on new hires, or on an ongoing basis for existing staff.

3. Governance (including risk management, compliance, and related party issues)

Objective: Assess the appropriateness of the risk management framework and ensure that all associated compliance practices are adequate with the relevant risks captured, monitored, and reported and that there is an appropriate, proactive risk culture which is linked to the corporate social responsibility policy.

Issues to be considered.

Review of Policies and Other Written Materials

- Company risk management framework including structure and reporting lines. At a minimum, the framework should address the following risks: operational, reputational, strategic, liquidity, investment, benchmark, capacity, and counterparty. Other relevant issues include the following.
    - Identify the regulator for the investment manager and confirm licenses.
    - Identify the key risks for the entity and how the entity monitors and reports these.
    - Identify key staff involved in the company risk management arrangements and their responsibilities and level of experience.
    - Identify if there is a committee dedicated to corporate governance issues.
- Current Compliance Plan (including a policies/procedure register), ensuring that it is up to date and is reasonable for the entity's business model.
- Conflicts of Interest Policy (including related party issues) and details of how conflicts are mitigated, monitored, reported, and managed.
- Review the Class Action Policy and details of the investment manager's default position in the absence of instructions from the asset owner.
- Incident Management Plan with details on how an incident is determined, reported and managed (internal and external). Such a plan should include, but not be limited to, escalation procedures, breaches, and any incident(s) which may indicate a broad operational weakness.
- Internal Controls Report, with ideally the last three years made available for review. Ensure details of internal controls and applications of procedures are identified and highlight any weaknesses/breaches. Understanding the nature and scope of the controls report and reporting lines is important (e. g., GS007, IAS 70 etc.).

- Trade allocation policy and details of the process to manage trades according to each mandate and pooled fund.

- Gift and Hospitality Policy with a gift/benefit register and details including any limits and pre-clearances and what would cause a breach.

- Review and assess the internal approach to corporate social responsibility and consider its implementation.

Qualitative Assessment and Observations

- An assessment of corporate culture implied by the Board and risk management framework. Assess if it is good practice and if not, where are the deficiencies. Check there is evidence of strong risk management to enable sound governance practice throughout the entity.

- Check the extent to which the corporate risk management and compliance culture permeates through the business, including support from senior management. Assess whether there are any potential or actual information barriers within the entity.

- Ascertain the attitude on the application of the various company policies. Ensure that staff understand what details are contained within the policies and why. Check that the content contained within the policies is part of the entity's operations.
- Ensure there is evidence and comfort that the investment manager complies with relevant laws and regulations within its jurisdiction. Check whether the investment manager has any previous or current issues with its regulator of which the RSE should be aware. Is all statutory reporting and taxation lodgement up to date by the investment manager.

- Check the investment manager is aware of the legislative environment within which it and the relevant RSE operates.

- Identify any risks that the investment manager is not adequately acknowledging or addressing.

- Assess the frequency of relevant policies being reviewed and evidence of such reviews.

Indicators of Good Practice

- Implementation of the 3-lines-of-defence model and a clear reporting and oversight structure.
- CRO or equivalent reporting directly into CEO and Risk Committee.
- Maintenance of a Governance, Risk and Compliance system as a tool to centrally manage and capture risks, controls, compliance attestations and governance registers such as incidents, breaches, and conflicts of interest.
- Dedicated internal audit team (either in-house or outsourced) is established to perform regular audit reviews based on a formal Internal Audit Plan across all areas of the business and geographical locations.
- Maintenance and regular review of formal Governance Frameworks/Policies including a Risk Management Framework and a Compliance Framework. Good practice is for such frameworks to outline a clear Board Risk Appetite Statement, key risk indicators, a clear risk management

strategy, a clear conflicts of interest policy and a compliance programme, that incorporates periodic testing.
- Regular review of risk register and assessment of risks within the business units and emerging risks.
- Regular reporting is completed by second line-of-defence teams to appropriate oversight Committees such as a Risk Committee and Audit and Compliance Committee (or equivalents).
- Regular Risk Culture Surveys are conducted, and participation rates are indicative of a strong risk culture.

Indicators of Poor Practice

- No documented compliance and risk framework, policies or procedures.
- No designated in-house compliance and risk management functions.
- Inadequate governance oversight from the Board and its committees – Board does not have formal Charter/Terms of Reference to define the roles and responsibilities or inadequate reporting to the Board from management or second line-of-defence teams
- No formal incident or breach identification, reporting and escalation processes.
- Inadequate monitoring, review, and assessment of Compliance obligations, e.g., personal trading, insider trading, gifts and entertainment restrictions
- Situations that could potentially result in conflicts of interest have not been identified, recorded and managed.
- Statutory and other regulatory reporting is not up to date or contains inaccuracy or inconsistency.
- Related party transactions that result in conflicts between the investment manager and the funds or investors.

4. Trading Processes and Operational Functions (including settlement and confirmations, trade allocation, cash movements, reconciliations, error management, segregation of duties)

Objective: To ensure the investment manager has appropriate trading policies and systems in place appropriate to the asset class, specifically addressing transparency, robustness, and effectiveness.

Issues to be considered.

Review of Policies and Other Written Materials

- Trade policies and processes including details of trade execution, trade confirmation, trade allocation and settlement, trade reconciliation, trade error policy, assessment and monitoring counterparties, brokerage allocation, derivatives policy and record keeping. Note that this process needs to be auditable with APRA specifically concerned to see that trade allocation is equitable with no client (including internal funds) receiving a disproportionate share of the best opportunities or prices. Particular attention is to be paid to any manual processes to ensure appropriate controls are in place.

- Cash controls including cash movements, authorisations, instructions to third parties and monitoring cash balances.

- Security of and the ability to identify individual assets. Such inquiry should account for assets held

in a discrete and/or pooled vehicle.

- Insider trading policy and policy in relation to personal trading.
- Policies in respect of dealings with (any and all) related parties, specifically looking for how potential and actual conflicts are identified, the process for managing any identified conflicts and the process for reporting to the RSE. Assess any soft dollar policies and the appropriateness of such policies.
- Policies relating to compliance breaches, incident management, fraud and corruption, and anti-money laundering provisions and policies.
- Policies on process to deal with proxy voting and corporate actions.
- Statements of the controls, roles, and responsibilities of personnel authorised to input and authorise transactions and reference to appropriate segregation of duties between investment and operational staff.
- Review of policies and processes to instruct custodians (ideally as straight through as possible via a recognised method of instructing (e. g., Swift or Custodian portal).
- Review of policies to conduct reconciliations including identification and frequency of trades. Review escalation and clearance processes, and timeframes for aged breaks as well as what primary and secondary sources of data are used.
- For mandates, documentation setting out procedures to ensure the mandate is established and monitored in accordance with the specifications in the governing client documentation (e. g., Investment Management Agreement, Service Level Agreement). Review the existence of any mandates issued by the investment manager that may impact the RSE.
- For pooled funds, documentation setting out name in which assets are registered and processes to register derivatives and any "unregistered assets".
- Recognise that Trading Processes, Operational Functions and Reporting may differ depending on the asset (listed vs unlisted/derivatives (OTCs) vs physical/ domestic vs global).
- Review and assess Trade Errors Policy and Remediation Policies.

Qualitative Assessment and Observations

- General review of all trading and operational processes for compliance with policies (as listed above).
- Confirmation that transactions are independently verified and that appropriate processes exist to ensure transparency and role segregation.
- Identification of any related party transactions and confirmation that any and all actual and perceived conflicts due to related party transactions are identified and managed by the investment manager via an arm's length and independent process.

- Review of trading and operational processes for risks of error in manual transactions. Review actions taken by investment manager when errors are identified.

- Ensure appropriate processes are in place to identify and rectify any failed trades or other recording errors and not repeat them.

- Spot check on corporate action processes to ensure compliance with policy.

Indicators of Good Practice

- Appropriate written policies and procedures for key trading and operational processes.
- Appropriate segregation of duties in order management, trade execution and trade management.
- Independent confirmation of transactions and reconciliation of balances.
- Pre and post trade compliance are monitored via a system (order management system). Coding of rules and any subsequent amendments should be done by non-Investment team.
- Pre-trade breach alert is not allowed to be overridden by investment personnel.
- Pre-trade breach is monitored and approved by non-investment personnel.
- Appropriate trading compliance breach management and escalation process.
- A process for allocating trades is in place for fair trade allocation opportunities between various clients.
- Trade or deal allocation outcomes are subject to formal oversight and review.
- Appropriate segregation of duties between cash instruction and cash payment functions.
- All processes involving manual intervention are subject to four eyes principle.
- A client is compensated for trade and process errors and formally documented in the Trade Error Policy.
- No threshold for communicating errors to investors.
- A compliance function responsible for the control and monitoring of best execution, including regular review of execution reports/records. The results from such review should be reported to the relevant committee, e.g., best execution committee, on a periodic basis.
- Pre-clearance is required for personal trading and is valid for short period (i.e., no more than 2 business days. Pre-cleared personal trading is reconciled with a transaction (broker statement).
- Personal trading policy is applicable to not only staff but also staff's related person such as spouse and dependents.
- Due diligence is performed on a broker prior to appointment and on a regular basis (e.g., annually)
- A committee approves a broker to the panel. Formal review of approved broker panel is performed on a regular basis.
- Good Cash Controls with All fund/client cash wires should be subject to at least two signatories/signatures, as required by the financial institution paperwork (prime broker, custodian, bank).
- Cash signatories should not include front office or marketing personnel and should not include those persons responsible for reconciling cash.

Indicators of Poor Practice

- No documented policies and procedures for key trading and operational processes.
- Inadequate segregation of duties and staff supervision resulting in fraud and asset misappropriation.
- Insufficient processes and controls to monitor IMA investment guideline rules, e.g., no pre-trade or post-trade compliance checks, unauthorised rule overrides.

- Compliance rules not automated within order management system.
- High level of manual processing across key trading functions.
- Inadequate controls around brokers/counterparty activities, fail trades and creditworthiness.
- Lack of documented processes and controls around trade errors reporting and rectification, incident management.
- Weak cash management controls, such as unauthorised cash movements, no separation of responsibility for cash controls and maintenance of cash records; outdated authorised signatory lists, long outstanding unreconciled items in accounts.
- Lack of transparency in the calculation and allocation of fees and expenses among investment vehicles.
- Qualified opinions and/or material exceptions relating to trading and operational processes are noted in the independent internal control reports (e.g., GS007 report)

5. Valuations

Objective: To assess the appropriateness of the valuation process, specifically assessing transparency, independence, robustness, and effectiveness at mitigating or removing the risk of errors in the valuation process of all relevant asset classes including listed and unlisted in liquid and illiquid markets.

Issues to be considered.

Review of Policies and Other Written Materials

- Review the methodology and appropriateness of valuations/pricing policies including the timing and frequency thereof (including suspended stocks), having regard for the specific asset class and instrument type (e.g., OTC derivative) under review.

- Extent to which any of the process is outsourced and a policy that covers this if this is the case. Statements of roles and responsibilities of staff involved, including appropriate independence, accountability, and segregation of duties.

- General review of all valuations and reporting processes for compliance with policies (as listed above) and relevant accounting standards and in line with appropriate guidance issued by industry associations.

- Review of valuation policy to ensure that it covers:
    - key processes for managing valuations (e.g., approval, rejection, and reassessment)
    - independent pricing of securities
    - triggers for out-of-cycle valuations
    - adequate management of stale prices
    - an appropriate valuation committee structure and internal governance to address complex valuation issues

- Personnel involved in the valuation process are independent and qualified.

- Review the process to appoint and rotate any external valuers.

- An assessment of whether there have been any unit pricing errors, near misses or compensation required and actions taken by the investment manager if these have occurred.

- If any aspect of this function is outsourced, review the process to select and monitor the service provider and its pricing system (e. g., oversight of their valuation policy, daily spot checks, reconciliation, review of certification, review of controls document). Similarly, where pricing feeds are used, ensure periodic formal review of pricing service providers and adequate monitoring of the effectiveness and accuracy of pricing feeds and the provider.

Indicators of Good Practice

- Valuation requires no subjectivity - there are detailed valuation policies with clear documentation of the valuation methodology, internal and external valuation processes, and controls.
- Evidence of back-testing of valuations with actual transactions.
- Regular reporting to the Board (or its delegate) to facilitate proper oversight of the valuation process, policies, and procedures, especially when there are significant changes to methodology.
- Periodic reviews by internal audit (or independent consultant) to assess the overall quality and effectiveness of the valuation management and compliance with the Valuation Policy.
- Valuation Committee in place for governance and monitoring securities valuations, including any delisted or hard to value securities. The majority of the Valuation Committee's members should be from non-investment functions.
- For Unlisted assets ensure assets and unit prices are held at Fair Value and independent valuations are appropriately reviewed.
- For unlisted assets, including the following: –
  - Independent panel of valuers who are rotated every three years at a minimum.
  - Desktop valuations issued monthly or quarterly.
  - Independent valuations issued annually, at a minimum.
  - Policies and/or procedures set out trigger events for the review of valuations to reduce the risk of stale values.

Indicators of Poor Practice

- Valuation methodology and process are not in line with applicable accounting practices and regulations.
- Inconsistent valuation practices and frequent methodology changes.
- Inadequate internal review and oversight process leading to inaccurate valuations.
- No valuation committee (or equivalent governance model) to provide governance and oversight.
- Lack of clear documentation, minutes and records of decisions.
- Inadequate documentation of the valuation policy and pricing processes and procedures.

6. IT Systems and Security

Objective: To ensure the investment manager's IT systems and security processes are appropriate for the asset class, region and marketplace in which it is investing and are sufficiently robust and fit for purpose and that it has the knowledge and capacity to continually develop these processes and security systems.

Issues to be considered:

Review of Policies and Other Written Materials

- Review any relevant IT systems and security policies with specific reference to IP (controls around

proprietary spread sheet analysis) and cyber risk and ensure compliance with the requirements of CPS 234.

- Specifically review the IT security policy. This should be detailed and include incident management procedures, an assessment of the physical security, firewalls, data encryption, password rules, external access, mobile devices, patch management, penetration testing and vulnerability assessment.

- Details on data security systems for both onsite and cloud-based servers, administration rights access, phishing, and processes for the oversight and assessment of key third-party service providers' cyber security environments.

- A mapping of the investment manager's overall IT infrastructure showing all systems (including manual), and relevant controls, used for the investment management functions. A review should also consider any interactions of systems of service providers with those of the investment manager and/or in-house systems.

- Details on the key data flows between the systems, the age of each of the key applications and whether any upgrades or enhancements are scheduled.

- Statements of roles and responsibilities of IT staff, specifically considering who is ultimately responsible for cybersecurity, level of seniority, potential conflicts, experience, and capability as well as the level of oversight including the role of the investment manager's Board. The adoption of a recognised framework (such as ISO, NIST etc.) should also be included in the assessment of capability.

- Assessment of procedures in place to limit the potential for intellectual property loss where a firm utilises multiple IT consultants.

- Review an attestation that cyber security testing is undertaken on a regular basis with satisfactory results.

- General review of all IT systems and security processes for compliance with policies (as listed above), including an assessment of whether they are fit for purpose for the investment manager's organisation, specifically its size and complexity.

- Review the coverage and adequacy of the IT security policy. The assessment should include an outline of the controls in place to secure applications hardware and infrastructure against unlawful access.

- Review how the IT infrastructure compares to industry peers and its ability to perform necessary tasks.

- Test the extent to which spreadsheets are used within the client operations, including their development and modification, the checking of inputs into the spreadsheets and understanding of the controls and approval processes.

It is important to be assured that the investment manager has the foresight to continually be alert to new risks (in particular cyber security risks) and be open to the development of new mitigation techniques and

security processes to guard against new risks and attempts to infiltrate systems.

Indicators of Good Practice

- Maintenance and compliance with IT/Security Frameworks that are aligned to best industry standards such as APRA CPS 234 Information Security, ISO 27001 and NIST Cybersecurity Framework.
- Completion of regular information security training to all staff including deployment of phishing campaigns.
- Maintenance and implementation of a clear testing program outlining various key testing activities completed throughout the year, which may include penetration testing, vulnerability assessment, SOC reporting, internal audit reviews, simulation exercise and phishing campaigns.
- Routine rotation of the third-party penetration testing service provider to ensure objective testing of existing security controls.
- Clear policies are in place around oversight and monitoring of third parties who manage the organisation's information assets.
- A robust information security incident management process is established to ensure timely detection and rectification of vulnerabilities, incidents, and breaches.
- Regular reporting on key information security metrics to appropriate oversight bodies such as an Information Security/IT Committee.
- Utilize VPN for remote work instead of home WIFI.

Indicators of Poor Practice

- No change management process in place for system upgrades/enhancements.
- Lack of documented 'front-to-back' data flows between systems across the organisation.
- Inadequate data security and privacy measures to protect personal or confidential and sensitive data resulting in unauthorised data access.
- Data storage environments are not fully secured. The potential risks and considerations associated with outsourcing data storage (e.g., in the cloud) are not fully understood and mitigated.
- There are no processes and controls to ensure data is kept and disposed of in accordance with business requirements and relevant legislative requirements.
- Independent internal controls report (e.g., GS 007) or ITGC report noted qualified opinions and/or material exceptions.
- Lack of experienced professionals (in-house or outsourced) overseeing IT and cybersecurity

7. Business Continuity

Objective: Assess the investment manager's BCP and be assured that it is appropriately tested and maintained.

Issues to be considered.

Review of Policies and Other Written Materials

- Review a copy of the Business Continuity Plan (BCP), specifically looking for details about business continuity in the event of a disaster (the Disaster Recovery Plan (DRP)), consideration of disaster recovery capacity planning, testing completed and frequency of testing.

- Review copies of BCP and DRP test reports.

- Specifically enquire about the following.

    - Cybersecurity incidents where the investment manager's email and files hosting are inoperable, unavailable or degraded.
    - A specific cybersecurity incident management response plan.
    - Cybersecurity insurance and levels/coverage.
    - Security incident (e. g., crime, demonstration) where their location works perfectly but staff cannot access it.
    - Phone and or internet outage of several hours or more.
    - IT failure at a key service provider such as Bloomberg, Custodian etc.
    - If there is a disaster recovery site, is access guaranteed, and what proportion of staff can work from the site for more than a certain period (e. g., two weeks, a month etc.)?

Qualitative Assessment and Observations

- Ensure an annual DRP test is carried out.

- Review the results of the most recent DRP, specifically looking for areas of weakness and rectification implemented or planned. Reviews should include scenario analysis and rectification policies and strategies.

- Assess the investment manager's inclusion of its critical service providers in its annual DRP test to ensure minimal disruption to its business in the event of an incident.

- Ensure the BCP Policy has been reviewed at least annually and regular training given to employees.

- Does the policy include the key Business Continuity Events, critical business activities, roles and responsibilities for the organisation.

Indicators of Good Practice

- A formal Business Continuity Management Policy is maintained and regularly reviewed. For good practice, the Policy is expected to clearly outline critical business activities, recovery objectives, key roles and responsibilities and response plans to plausible disruption scenarios.
- A dedicated Crisis Management Team (or equivalent) is established.
- Business continuity related roles and responsibilities are included in job descriptions and performance plans.
- Governance of the business continuity programme is regularly reviewed by the governing body at pre-agreed intervals or following significant change.
- Maintenance and implementation of a clear testing program outlining various key testing activities completed throughout the year, which may include a failover exercise, loss of IT facilities, building evacuation exercise and back up recovery exercise. Tests are completed to ensure recovery objectives are met.
- Solutions and plans are reviewed periodically or after stipulated trigger events. Realistic testing should be conducted to confirm the adequacy of the investment manager's response strategies.
- An effective internal and external communication strategy has been developed.

Indicators of Poor Practice

- Inadequate coverage of extreme events/scenarios and associated response plans resulting in the investment manager's inability to operate in the event of a disaster.
- Lack of evidence that the BCP/DRP is being reviewed and tested regularly.
- Material weaknesses/issues identified in the BCP/DRP testing or independent internal controls report (e.g., GS 007) are not addressed in a timely manner.
- No cybersecurity insurance coverage or evidence of any other controls that reduce the consequence of a cybersecurity incident.
- No evidence of periodic cybersecurity testing and/or cybersecurity awareness training and phishing email test for staff.
- Poor controls and support for remote working arrangements.

8. Service Provider Oversight

Objective: Assess the extent to which the investment manager has outsourced services and that these are adequately documented and managed.

Issues to be considered.

Review of Policies and Other Written Materials

- Review of any and all policies that relate to any current or prospective material outsourced arrangements. The key material outsourced arrangements that could be in place include Custody, IT, Middle Office, Fund Administration, Prime Brokerages and Unit Registry. However, there may be others, and these should be identified by the ODD provider.

- List of any current material relevant to outsourced arrangements, including firms by name and what services are provided to the investment manager (e. g., Service level Agreement ('SLA') with Custodian).

- Review any policy regarding counterparty risk and the implications for the RSE (e. g., Derivatives Policy, Currency Policy).

- Assess the oversight by the investment Manager of major third-party vendors. Such an assessment should include updates, controls and monitoring of third parties such as Custodian, Administrator, broker services, technology providers arrangements

- Assess the extent to which the investment manager monitors and reviews counterparty risk on a periodic basis.

Qualitative Assessment and Observations

- Review the services outsourced and comment on whether these are fit for purpose i. e., is it appropriate that the investment manager has outsourced these arrangements. Comment on the firms to which the outsourced services have been allocated and whether they seem reasonable

or not.

- Ensure that the investment manager has appropriate due diligence processes for service provider selection and appointment (e. g., Auditor).

- With respect to oversight of the provider, ensure that the investment manager has an SLA (or equivalent) in place, consider how it is monitored (including on-site visits to the outsourced provider(s)), with what frequency and the extent to which the detail of the monitoring is documented and recorded.

- Assess the willingness/ability of the investment manager to take appropriate responsibility for the actions of their outsourced provider(s) through provisions in the Service Level Agreement. Assess the robustness of the Service Level Agreement between the investment manager and the outsourced provider(s).

The Report should identify any key issues of relevance for an RSE in any agreements and key SLAs between the investment manager and the service provider.

Indicators of Good Practice

- A formal Outsourcing Policy (or equivalent) is maintained and regularly reviewed, which should include contingency plans and exit strategies.
- Clear governance and oversight of relationships with key/material third parties.
- A service and performance review and monitoring process is clearly outlined and implemented throughout the year. This includes both formal (for example deep-dive reviews across various areas of the service provider's business) and informal reviews (for example regular SLA monitoring and reviews).

Indicators of Poor Practice

- Service providers do not have the appropriate qualifications and capabilities to meet business requirements.
- Non-independence of service providers and potential for conflicts of interest.
- No formal documented service provider screening, selection, and monitoring processes.
- Lack of formal measurement/monitoring of SLA and incident management process

9. Reporting

Objective: Assess the quality of existing reporting, its timeliness and compliance with regulatory requirements as appropriate.

Issues to be considered:

Review of Policies and Other Written Materials

- Policies and/or processes on approach to reporting to clients (including the independence of reports, timeliness, clarity, and detail).

- Ability to recognise and report mandate breaches.

- Reporting on Corporate Responsibility, Modern Slavery and Proxy voting records available.

Qualitative Assessment and Observations

- Determine if reports are automatically/system generated or manually prepared and the security of the delivery mechanism.

- Assess capabilities and systems for timely and accurate delivery of reporting.

Indicators of Good Practice

- Timely and compliant reporting to regulators (both statutory reporting and breach reporting).
- Timely notification to clients on incidents and breaches (both mandate breaches and operational incidents/breaches).
- Detailed process and automation are in place to detect mandate breaches such as pre-trading and post-trading compliance checks with any flags requiring review by an independent compliance team.
- Automated system generated reporting with no manual intervention.

Indicators of Poor Practice

- Lack of transparency resulting in inaccurate/incomplete/inconsistent information being reported.
- No evidence of segregation of duties and review across report production.
- No tracking of deadlines across reporting obligations to clients.
- History of regulatory fines or warnings for late or incorrect filings.

10. Environmental, Social & Corporate Governance

Objective: To assess the sustainability and social impact of the investment manager's corporate operations (which contrasts with the specialist investment function which assesses an investment manager's skills and expertise for investing funds within ESG parameters).

Issues to be considered.

Review of Policies and Other Written Materials

- Policies and/or processes on approach to obtaining and ensuring diversity of team members, senior leadership, Board / Committees (could separately be covered in personnel section of operations due diligence).

- Policies and/or processes on approach to sustainable environmental impact for the operations of the investment manager's business

- Policy addressing investment manager's approach to the incorporation of environmental, social and governance (ESG) factors within the investment process (if applicable).

Qualitative Assessment and Observations

- Determine if the investment manager has written diversity targets and calculate whether those targets are met. Review the steps taken to bridge any gaps and assess whether those steps are likely to achieve the target. Consider whether the target is too low.

- Determine if the investment manager has carbon neutral targets and calculate whether those targets are met. Review the steps taken to bridge any gaps and assess whether those steps are likely to achieve the target. Consider whether the target is too low.

- Evidence of processes and controls for monitoring and reporting of ESG incidents.

Indicators of Good Practice

- Clear ESG Policy (or equivalent) is maintained and reviewed regularly for the operations of the investment management business. For good practice, it is expected that such policies are aligned with relevant responsible investing frameworks such as APRA CPG 229 Climate Change Financial Risks and recommendations under the Task Force on Climate-Related Financial Disclosures.
- ESG metrics and thresholds are established and regularly monitored for the corporate operations of the investment manager. Good practice includes a commitment to being carbon neutral in the next twelve months including staff travel to and from work and to and from client's meetings and events.
- ESG of the investment manager's operations is embedded into the organisation's Risk Management Framework and is regularly monitored by senior management.

Indicators of Poor Practice

- Inadequate processes and procedures around the establishment, monitoring and reporting of ESG KPIs, resulting in negative media coverage and reputational risks.
- Examples of social red flags (e.g., human rights issues, gender discrimination, forced labour) and governance problems (e.g., bribery and corruption).
- Insufficient controls around modern slavery, including not having a Modern Slavery Statement if applicable

11. Data Governance & Management

Objective: To assess the quality and governance of data used, transmitted, and translated to support the investment decision making.

Issues to be considered.

Review of Policies and Other Written Materials

- Policies and/or processes on approach to Data Quality / Governance (setting out data roles and responsibilities)

- Policies and/or processes for assessing data confidentiality

- Policies and/or processes for transmitting data between organisations

- Policies and/or processes for the systematic review of data quality before using data in decision-support models or reporting

- Policies and/or processes in relation to developing models in spreadsheets or similar tools.

Qualitative Assessment and Observations

- Determine if key decisions are being made using from tools which are not systemised. Is there a whole-of-firm policy on how to build, maintain, secure, access spreadsheet models? How does the firm ensure adherence to that policy? Is there staff training for how to build spreadsheet models?
- Is there a register of critical models / spreadsheets, and is each model regularly assessed for key person risk and other relevant risks (as part of the investment manager's broader risk management framework)?

Indicators of Good Practice

- A formal data governance policy or equivalent in place,
- The policy should dictate data classifications, password policies, and any controls in place to limit sensitive information leaving the business and going to unauthorised people.
- Good practice is to avoid sending sensitive data via email, a secure method should be used in the first instance.
- Alignment to General Data Protection Regulation ('GDPR') by investment manager,,, or equivalent.
- Clear data accountabilities and ownership structures across Business, Technology and Projects.
- Clearly documented and operational policies, procedures/ standards for ensuring ongoing oversight and governance of critical data in accordance with agreed ways of working. Preferably aligned to industry leading frameworks including CPS234, CPG235 and the Enterprise Data Management Council's latest Data Management Capability Model.
- Clearly documented understanding and prioritisation of the data critical to business processes and decisions. How critical data is collected, processed, and shared across upstream processes and systems.
- Clearly documented understanding of the data quality requirements for critical data
- Evidence of ongoing assessment and verification that critical data is fit-for-purpose
- Established / standardised processes to investigate and remediate instances where data is not fit-fit-for purpose.
- Internal Auditing / Assurance of adherence to policies, procedures /standards and agreed ways of working.
- Embedding of preventative controls to address systemic data issues.
- Scope covering operational data management as well as reporting and analytics.

Indicators of Poor Practice

- There is no data governance framework or policy that specifies all relevant regulatory requirements and defines clear responsibilities for data, e.g., there is no central responsibility for data governance and management.
- Data maturity assessment has not been undertaken to identify the core data-related issues that need to be addressed to support business outcomes.
- Poor data quality due to unclear definitions of data fields and missing "golden record" master data.

- Data quality management is not appropriately addressed - there are inadequate processes and procedures in place to monitor the accuracy, completeness, timeliness, consistency, and reliability of the data.

Attachment 1

Suggested Sample Covering Letter

To whom it may concern

This has been prepared in accordance with the *Investment Manager Operational Due Diligence Guidance Note* prepared by AIST and dated May 2022

"ODD Provider" confirms that it is independent of "Investment Manager", has conducted this due diligence on a completely independent basis and has received a fixed dollar fee for its services.

"ODD Provider" has reviewed the operational framework, functions, and processes of "Investment Manager" via the following means.

- A desktop review of policies and procedures as provided by "Investment Manager".
- Additional questionnaires prepared by "ODD Provider" seeking extra information and/or clarification.
- A review of policies and procedures against actual processes in the business via interviews, inspections, and other on-site methods.

"ODD Provider" confirms that "Investment Manager" can provide this Summary Report to any RSE that is a current client or a prospective client. In receiving this Summary Report, an RSE acknowledges that there are elements of judgment in the due diligence conducted by "ODD Provider" and that no matter how well designed and implemented a review process is, it can only provide reasonable, but not absolute, assurance regarding "Investment Manager's" policies, processes, procedures, and controls with respect to the management of operational risk.

Signed by:

XYZ Authorised representative of ODD provider

Date: