AIST
Investment Manager Operational Due Diligence Guidance Note
February 2017

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* (http://www.apra.gov.au/Insight/Documents/14-Insight-Issue-1.pdf), it first did so in relation to operational due diligence (ODD) on investment managers. There have been a number of subsequent occasions at conferences and in other forums where APRA has made its expectations clear, drawing RSEs' attention to the need for, and importance of, ODD. APRA reminded RSEs that, going forward it will assess their processes undertaken for managing both investment and operational risk when appointing investment managers/investing in external products.

The need for investment due diligence, including examining the investment philosophy and process, portfolio composition and performance of the investment manager and the relevant products is well recognised. Also of great importance, but frequently receiving less attention until now, is the need for operational due diligence on the investment manager/product. This is 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.

RSEs have a legal obligation to comply with APRA's requirements.

Investment Manager Operational Due Diligence Review Process

AIST, via a dedicated Working Group of RSE representatives, has developed this Guidance Note 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 meet its regulatory requirements.

The ODD review process must be conducted by an appropriately qualified, reputable, competent firm that is independent of the investment manager/product. AIST is not in a position 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 firm conducting the ODD.

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 organisation. That is, this is not a "tick the box" exercise and it is expected that the ODD provider expresses an independent validation of the investment manager's attestation regarding its policies and practices. As a result, AIST expects that the ODD review process will 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 for additional inquiry depending on the investment manager/product under review.

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 Guidance Note as the basis for review. This will create a cost effective, streamlined process which will help the RSE licensees assess operational and associated risks when deciding on the appointment of a manager.

AIST's preferred outcome of the ODD review process is for the ODD provider to prepare a Summary Report which outlines any Operational Risk(s) to be considered when appointing an investment manager. AIST acknowledges that there may be variation in the Summary Report (The Report) which will depend on the firm chosen to conduct the ODD review. The Report will be provided to the investment manager by the specialist ODD firm, and, similar to the process for the GS007 for example, the investment manager will make The Report available to existing and prospective clients on request. RSEs will require an updated Report on an annual basis and it is expected that the investment manager would provide the same on this basis.

General Requirements in this Guidance Note

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

- Organisation Structure;
- Personnel;
- Governance (including risk management, compliance and related party issues);
- Trading Processes and Operational Functions (including the ability to identify individual assets, settlement and confirmations, trade allocation processes, reconciliations, segregation of duties and registration of assets);
- Valuations;
- IT Systems and Security;
- Business Continuity and Disaster Recovery;
- Service Provider Oversight; and
- Reporting.

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.

AIST has developed this approach in order 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 investment risk prudently whilst doing so in the most economic and efficient manner.

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

AIST Working Group
Contact: Tom Garcia, CEO, AIST
tgarcia@aist.asn.au

1 Organisation Structure

In conducting ODD at the organisation level, it is expected that the following issues will be considered.

Review of Policies and Other Written Materials/Desktop Due Diligence

- 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.

- Board Structure including committee membership, roles and responsibilities.

- 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 outsourced providers. *(Note that more detail is specifically requested on a number of these areas later in this Guidance Note)*

- Reference to the total funds under management by product, and any capacity issues.

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

- Review audited financial statements.

- Board and Committee structures and role statements.

- Confirmation in writing that they have professional indemnity, electronic and computer crime fraud insurance with copies provided. The level of insurance cover should be noted.

On-site/More Detailed Due Diligence

- 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 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 Report should review 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 on the risk culture to ensure that this message is set from the top and permeates the organisation appropriately.

2 Personnel

In conducting ODD with respect to personnel, it is expected that the following issues will be considered.

Review of Policies and Other Written Materials/Desktop Due Diligence

- Company Code of Conduct (or other standard on ethical/professional behaviour) and all related policies.
- Biographies of all key personnel, ensuring that background checks, 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 are provided. 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.
- Remuneration policies, staff training and retention/succession planning policies.
- Team management policies and processes to ensure appropriate staff coverage at all times.
- 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.

On-site/More Detailed Due Diligence

- 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.
- Examine the linkages between performance and remuneration to ensure that incentive structures are appropriate and in the clients' best interests.
- Review the personal trading policy and test the appropriateness for the nature of the relevant mandate; and also 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.

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.

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

In conducting ODD with respect to governance, it is expected that the following issues will be considered.

Review of Policies and Other Written Materials/Desktop Due Diligence

- Company risk management framework including structure and reporting lines. At a minimum, the framework should address the following risks, operational, reputational, strategic, liquidity, investment, 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.
- 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 breaches, but include any incident 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 and 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.
- Hospitality Policy with a gift/benefit register and details of what is acceptable and what would cause a breach.

On-site/More Detailed Due Diligence

- 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 a 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. Has the investment manager had any issues with its regulator of which the RSE should be aware?

- 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.

The Report should review the appropriateness of the risk management framework and ensure that all associated compliance practices are adequate with the right risks being captured, monitored and reported, and that there is an appropriate, proactive risk culture.

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

In conducting ODD with respect to trading processes and operational functions, it is expected that the following issues will be considered.

Review of Policies and Other Written Materials/Desktop Due Diligence

- Trade policies and processes including details of trade execution, trade confirmation, trade allocation and settlement, trade reconciliation, trade error policy, dealing with 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 handling including cash movements, authorizations, 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.

- 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 roles and responsibilities including details 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 documents 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 side letters issued by the 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".

- Recognize that Trading Processes and Operational Functions may differ depending on the asset (listed vs unlisted/derivatives (OTCs) vs physical).

On-site/More Detailed Due Diligence

- 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.

The Report should review the appropriateness of the operating model employed, specifically assessing transparency, robustness and effectiveness.

5 Valuations

In conducting ODD with respect to valuations, it is expected that the following issues will be considered.

Review of Policies and Other Written Materials/Desktop Due Diligence

- Review of valuations/pricing policies including the timing and frequency thereof (including suspended stocks).

- 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 and segregation of duties.

On-site/More Detailed Due Diligence

- General review of all valuations and reporting processes for compliance with policies (as listed above).

- Review of valuation policy to ensure personnel involved are appropriately independent and qualified, that there is independent pricing of securities, that there is adequate management of stale prices and that there is an appropriate valuation committee structure and internal governance to address complex valuation issues.

- 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, what is done to 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 adequate monitoring of the effectiveness and accuracy of pricing feeds and the provider.

The Report should review the appropriateness of the valuation process, specifically assessing transparency, robustness and effectiveness at mitigating or removing the risk of errors in the valuation process.

6 IT Systems and Security

In conducting ODD with respect to IT systems and security, it is expected that the following issues will be considered.

Review of Policies and Other Written Materials/Desktop Due Diligence

- Review any relevant IT systems and security policies with specific reference to IP (controls around proprietary spread sheet analysis) and cyber risk.

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

- A diagram 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, 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.

On-site/More Detailed Due Diligence

- 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.

The Report should review the appropriateness of the IT systems and security within the organisation, specifically assessing whether they are robust, sufficient and fit for purpose for the investment management strategies offered by the investment manager.

7 Business Continuity

In conducting ODD with respect to business continuity, it is expected that the following issues will be considered.

Review of Policies and Other Written Materials/Desktop Due Diligence

- 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)), existence of disaster recovery sites, testing completed and frequency.

- 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, phone outage 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 of time (e.g. two weeks, a month etc.)?

On-site/More Detailed Due Diligence

- 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.

The Report should review the investment manager's BCP and be assured that is appropriately tested and maintained to ameliorate any concern for an RSE.

8 Service Provider Oversight

In conducting ODD with respect to service provider oversight, it is expected that the following issues will be considered.

Review of Policies and Other Written Materials/Desktop Due Diligence

- 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 (eg. SLA with Custodian).

- Review any policy with regard to counterparty risk and the implications for the RSE (eg. Derivatives Policy, Currency Policy).

On-site/More Detailed Due Diligence

- 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 (eg. Auditor).

- With respect to oversight of the provider, ensure that the investment manager has a Service Level Agreement (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 details 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 determine the extent to which the investment manager has outsourced any material services and the extent to which these are appropriately documented and managed. 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.

9 Reporting

In conducting ODD with respect to reporting, it is expected that the following issues will be considered.

Review of Policies and Other Written Materials/Desktop Due Diligence

- Policies and/or processes on approach to reporting to clients (including the independence of reports, timeliness, clarity and detail).
- Review of sample reports.
- Ability to recognize and report mandate breaches.

On-site/More Detailed Due Diligence

- Determine if reports are automatically/system generated or manually prepared.
- Spot checks on sample reports for accuracy and timeliness.

The Report should determine that the investment manager can provide accurate and adequate reporting to an RSE in a timely manner, such that *inter alia* the RSE can meet its reporting obligations to APRA and any other regulator as well as meeting its own reporting requirements.

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 June 2016.

"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: