Guidance Note

Investment Management Operational Due Diligence Guidance Note

2025

Table of contents

A About ASFA Guidance Notes

ASFA Guidance Notes are intended to provide superannuation trustees (trustees) and funds with information and guidance about ways of doing things that work and benefit members and the superannuation industry.

Guidance notes recognise that one size does not fit all. They set out better practice gleaned from ideas and experience from those who have undertaken similar activities in related fields.

Each of ASFA's member organisations covers a diverse range of goals, member needs and resources according to which they can adapt this Guidance Note's recommendations to their own particular circumstances.

This Guidance Note is intended as a guide only and is not intended to be used as a substitute for professional advice. The Association of Superannuation Funds of Australia Limited expressly disclaims all liability and responsibility to any person who relies, or partially relies, upon anything done, or omitted to be done, by this publication.

A.1 Background to this Guidance Note

This Guidance Note ('the GN') leverages former industry discussion and collaboration undertaken in producing Australia's first GN for Operational Due Diligence (ODD). It builds on, and replaces, an earlier note developed by a Working Group of Registrable Superannuation Entities (RSE) representatives for the former Australian Institute of Superannuation Trustees (AIST).

Recognising its benefit to a broad group of industry participants, ASFA has agreed to continue guidance on ODD matters going forward. In doing so, the former AIST GN has been substantially updated by a dedicated Working Group of ASFA member organisations, comprising JANA Investment Advisers, Mercer, IFM Investors, Robeco, NGS Super, Australian Retirement Trust, Hesta, and Gilbert + Tobin.

ASFA acknowledges the work of the former AIST Working Group in establishing the original GN and welcomes the opportunity to adopt and update it to provide continued guidance to the industry.

A.2 Regulatory Requirements

This GN does not seek to repeat or duplicate all relevant legislation or additional standards set by regulatory instruments relevant to investment management operational due diligence. Where they overlap or are inconsistent with this GN, the legislation or regulatory instrument will prevail.

The GN also does not attempt to clarify how obligations imposed by legislation or regulatory instrument work in practice. While this GN recommends practices which may support these obligations, it does not attempt to align or link practices to those obligations.

Nevertheless, some regulatory context is warranted.

- All RSE licensees are required by superannuation law to exercise care, skill and diligence in connection with their roles. The ODD guidance outlined in this GN would assist with demonstrating that care, skill and diligence has been exercised, noting that the requirements of that duty are broader than initial and ongoing due diligence.
- Certain APRA Prudential Standards such as CPS 230 and CPS 234 (which are explained further below) impose additional requirements in connection with material service providers engaged by RSE licensees and these requirements will potentially apply to investment managers, as well as to other entities that manage information assets of RSE licensees. Aspects of the guidance within this GN will

assist with demonstrating compliance with these requirements, noting that these prudential standards also require steps to be taken outside of the ongoing due diligence context.

As such, it is important to understand that this GN is not merely about compliance with CPS 230 and CPS 234, and compliance with those prudential standards requires action that is beyond the scope of this GN.

CPS230 Operational Risk Management

The Australian Prudential Regulatory Authority ('APRA') now routinely assesses RSE processes for managing both investment and operational risk when appointing and monitoring existing investment managers/investing in external products.

Effective 1 July 2025, APRA's, *Operational Risk Management Standard* (CPS 230) provides updated requirements to RSEs (in addition to other APRA-regulated entities captured under the cross-industry standard) with regard to managing operational risk. CPS 230 seeks to further uplift industry practice, recognising that operational risk is a whole of RSE initiative. ASFA recognises that reference to the outcomes of this GN may support RSE executives' completion of their obligations under the Financial Accountability Regime.

CPS 230 requires investment managers identified by RSEs (and some other asset owners) as being material to its operations to meet additional operational requirements. These requirements are in addition to the operational due diligence review practices discussed in this GN. To help ASFA members and investment managers identified by RSEs / asset owners as material, a supplement to this GN, specifically addressing the requirements of CPS 230, is located in Appendix 1.

A.3 Commencement

The GN is effective 1 July 2025, though it can be utilised prior to this period given its alignment with the prior standard SPS 231, *Material Outsourcing*. ASFA encourages trustees and interested parties to adopt (where not already in place) the guidance as soon as possible.

The ASFA Working Group will review this GN periodically to ensure it remains relevant and up to date.

Contact: Policy@superannuation.asn.au

B. Operational due diligence

B.1 Introduction

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 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. Furthermore, Prudential Standard SPS 220 Risk Management ('SPS 220') emphasises the obligation to have an appropriate risk management framework addressing all material risks.

[1] APRA Insight No.1 2014

The ODD review should be viewed as a process to identify and rate the operational risks of engaging/retaining an investment manager and is one component that forms part of the overall evaluation of an investment manager. For example, this GN focuses on operational matters, but an investment manager's historical actual (or, for new managers, synthetic) performance would be relevant inputs into an appointment decision. Similarly, the ongoing monitoring of an investment manager's performance would consider return and risk outcomes, as well as compliance with mandate restrictions and other contractual obligations, which are important aspects that are beyond the scope of the operational due diligence canvassed in this GN.

Importantly, the risks identified through the process should be considered through each RSE's own Risk Appetite Statement, noting that risks may be deemed reasonable for one RSE and inappropriate for another on this basis, recognising the fundamental role that a Risk Appetite Statement plays in determining appropriate risks based on each RSEs individual circumstances.

The review undertaken may be sufficient for some RSEs, while other RSEs may choose to perform additional operational due diligence activities to support the investment manager appointment decision and / or subsequent review. It is ultimately each individual RSE's responsibility to determine the acceptable level of risks, and to determine alignment of investment appetite relative to investment and operational risk periodically.

Common reasons and factors why different RSEs may take different views on materiality and the extent of the necessary operational due diligence include the following:

- the size and materiality of the proposed mandate may be different (in absolute terms or relative to the size of the fund or asset class)
- the type of investment strategy and the RSEs assessment of the materiality of the operational risks associated with the strategy
- differences in the scope of services to be provided (for example, not all investment managers will be authorised to transact in derivatives or to manage proxy voting and class action participation, which changes the scope of the relevant operational due diligence)
- the RSE's familiarity with the jurisdictions in which the investment manager and its fourth parties operate
- the ease with which the RSE could replace the investment manager, for example, by reason of having other comparable investment managers already appointed
- the resources available to the RSE to monitor and react to any incidence of issues of the kinds canvassed in this GN
- risk-based judgments on materiality and the extent of the operational due diligence that an RSE licensee exercising care, skill and diligence would undertake in the circumstances.

This GN provides suggested ODD review criteria that can be applied to pooled investment vehicles and Investment Management Agreements ('IMAs') and covers all asset classes, both listed and unlisted. In the same way that each RSE licensee needs to form a view as to whether CPS 230 applies to particular investment managers acting under an IMA, each RSE licensee should form a view as to whether CPS 230 applies to investments in pooled vehicles. That said, the statutory duty to exercise care, skill and diligence applies to decisions to enter into IMAs and invest in pooled vehicles.

This GN provides the industry a baseline reference for the ODD. ASFA recognises that the way in which ODD is being completed by RSEs is evolving rapidly and that there is no one 'right' model. Models within the industry range from:

- self review, where the RSE's inhouse teams complete operational due diligence
- combination review, where the RSE utilises in house teams to complete the operational due diligence complemented by external provider(s)
- fully outsourced, where the RSE utilises external providers to complete the operational due diligence.

Each model requires consideration for how the outcomes of the operational due diligence review is managed internally.

In Australia, it is recognised that an investment manager is expected to have its own ODD review completed by a reputable third party, commissioned by the investment manager, and is able to be used by the investment manager for:

(a) its own self-improvement; and

(b) to give current and prospective clients comfort with regards to a standardised set of operational requirements.

Alternatively, the GN can be used by a RSEs team to evaluate its investment managers, including internalised asset management.

A note to Investment Managers: *ASFA recognises that investment managers are not APRA regulated and therefore not directly captured by CPS 230, however, many of their Australian investors are. In addition, investment managers, their clients and prospects have found benefit in the output of ODD reviews. This GN provides a baseline that can be applied globally for coverage of key assessment criteria in an operational due diligence review process.*

Notwithstanding this, various regions around the globe may have specific nuances and different levels of best practice. A good operational due diligence reviewer will take this into account, while also providing feedback to the manager on what global best practice can look like.

B.2 Guidance Note structure

In recognition of the changing regulatory environment, this GN has been separated into enterprise and investment type categories, to make it easier for investment managers and providers to provide more focused information. This structure may also remove duplication in annual processes where no change has occurred and this can be attested to by the Investment Manager.

Topics are addressed in this GN as follows:

Topic	**Enterprise level**	**Listed asset classes / open ended pooled funds**	**Real asset classes / closed ended pooled funds**
	GN section	**GN section**	**GN section**
Organisational Governance	C.1		
Personnel	C.2		
Governance	C.3		
Trading and operations		C.4	C.5
Valuations		C.6	C.7
IT Systems and Security	C.8		
Business Continuity and Disaster Recovery	C.9		
Service Provider Oversight	C.10		
Environmental Social and Corporate Governance		C.11	C.11
CPS230	Appendix 1		

Reviewers should use their skilled judgement in determining which non-enterprise discussion questions are required.

Specific recognition has been paid to areas which face into both the enterprise/corporate and the strategy level of an investment manager. As an example, the corporate behaviour regarding to ESG is of interest, as is how a client's ESG choices are implemented in a specific strategy. This also applies to data, and in some cases, to service provider oversight. These principles may change in time as updated practices and requirements emerge. The process to develop the ODD Report will require consideration of each of the above areas. This approach has been developed to streamline the ODD review process. However, any RSE reserves the right to undertake their own ODD of investment managers and the provision of an ODD Report to an existing or prospective client should not preclude this from happening.

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

Private Company assets, investment directly into a non-trading company (such as a Pty Ltd)

For the avoidance of doubt, these guidelines are focused on operational aspects of investment managers as a service provider (provider of investment management services) to a Fund. They are not intended to apply in instances where there is a direct investment into an entity, although some aspects of operational due diligence would be considered as part of the investment and financial due diligence of the entity being invested into.

Crypto and associated asset types

These guidelines are not designed to specifically cover crypto currency and digital assets at this stage. RSEs and Asset Owners should complete additional due diligence should this be required. Investments in these assets potentially raise idiosyncratic legal and operational issues, including in relation to whether RSE licensees have power to make these investments or to authorise others to make these investments in their behalf. Those issues should be considered in relevant circumstances, but are beyond the scope of this GN.

B.3 Investment Manager Operational Due Diligence Review Process

The ODD review process must be conducted by an appropriately qualified and experienced professional / ODD Provider that is independent of the investment manager and has the appropriate skills to provide a meaningful, qualitative and quantitative report. As noted in Section B.1, ASFA recognises that this reviewer is equally as likely to be an in house team or an external provider.

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. Industry best practice is that an audit team is not best placed to complete this review, given its focus on peer relative best practice, despite the evidentiary nature of the reviews. ASFA discourages Investment Managers from utilising their audit firm to complete this review, due to separate skillsets and the utility of having an independent assessment.

It is expected that all 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, including professional relationships (such as audit). The degree of disclosure is at the discretion of the independent reviewer.

APRA has been clear in its communication with RSEs that the risk culture within an investment management organisation is highly important, particularly when it is a material outsourced third party provider. 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 in its assessment of the investment manager's operational risk profile. ASFA expects that the ODD review process should include a mix of desktop policy reviews, questionnaires and detailed on-site due diligence.

ASFA notes 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 – rather the two reports are complementary.

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

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 an input and part of the information used by the Trustee to manage its operational risk in line with the RSE's overall risk appetite.

B.4 Outcome of the Investment Manager Operational Due Diligence Review Process

The use of prior versions of this GN has created a consistent, streamlined process which will helps RSE licensees assess operational and associated risks when monitoring/deciding on the appointment of / ongoing investment in an investment manager. Investment managers choosing to support their current and prospective clients, including APRA-regulated clients, can assist by asking providers of ODD services to use this GN as the basis for review.

ASFA'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/retain an investment manager specific to defined investment strategies. ASFA 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, in turn to existing and prospective clients on request, as well as their service providers.

While ASFA cannot impose a requirement upon Investment Managers with regards to the use of the output from an ODD report, it is hoped that the Manager will benefit from the information with in it. As an example:

- a peer relative risk lens
- feedback into its business processes with a view to improvement
- integration into risk processes and improvement
- the ability to use the document with current and prospective clients regardless of whether the asset owner is regulated by APRA or based in Australia.

As part of the prudent oversight of investment managers, RSEs should carry out ongoing due diligence to the extent considered necessary to remain satisfied with the management of operational risks in connection with, and by, the investment manager.

Typically, RSEs will receive the following under the terms of their investment management agreements in the ordinary course of business:

- breaches of the mandate
- details of regulatory investigations
- changes in key personnel
- changes in ownership or organisation structure
- annual insurance certificates of currency
- annual GS007 (or equivalent) report
- Annual BCP test certificate or results summary

- annual Information security assurance reports.

These are important parts of ongoing operational due diligence. Judgement can be exercised in determining the extent of any additional information that should be obtained and the frequency for seeking that information. RSEs may take into account materiality, manager-specific concerns, industry thematics and other risk-based considerations in exercising their judgement to conduct additional due diligence at any point during the relationship.

Best practice would typically include annual on-site meetings (or video conferences) with investment managers to discuss significant changes concerning the manager, their business and their procedures which can form part of ongoing operational due diligence and may identify areas requiring further due diligence. In cases where an existing investment manager is appointed to manage an addition mandate, consideration should be given to any operational due diligence topics that are relevant to the proposed new mandate which may not have been previously considered.

C. Guidance

C.1 Organisational structure and ownership – corporate / enterprise

Organisational structure and ownership – corporate / enterprise

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 on the existence of a robust risk culture across the investment manager's entire organisation.

Scope	Examples of policy/documents	Examples of qualitative assessment and observations	Examples of good practice
Corporate structure • Legal structure (including any subsidiaries / related parties and their relation to the investment manager) • Ownership, equity and controlling interest (plus REM structure for equity holders) • Affiliated businesses and ultimate owner of the investment manager and any conflicts • Board and Committee structures	• A copy of an Australian Financial Services Licence, or relevant certificate of incorporation, local registrations etc • Equity shareholder agreements (if available) • Charter / Terms of Reference	• Ensure the ownership and legal structure is reasonably appropriate for the entity's business model • The organisational structure and staffing are appropriate, including operational support for the investment strategies and assets under management • 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. • Evidence of demonstrable roles and responsibilities.	• A clear organisational structure diagram is maintained and provided • Boards and Board Committees include independent representation • 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 • Consideration to skills matrices and DEI in structures at senior levels

• Financial stability • Business strategy (including any future business developments), additional office locations	• Review audited financial statements (three years then annually) • 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 • Copy of the AFSL or appropriate licence	• Reference to growth in assets under management (AUM), and any overall capacity issues, including client numbers, concentration and risks relevant to the business • Viability as an ongoing concern, profitability and operating above break even considerations	• The firm is financially stable to operate as a going concern. Where there has been a material drop in AUM (over 20% in the last year), the firm has sufficient capital resources to cover its cost base • The firm's investors base (in terms of investor concentration and investor type) is diversified • The firm has a formal budgeting process and senior management monitors ongoing income and expenditure against budgets
• Insurance coverage	• Copies of certificates of currency and limits	• The investment manager has professional indemnity, electronic and computer crime insurance coverage with copies of certificates of currency provided, including how cyber insurance has been considered • Adequacy of insurance coverage, renewal cycle and frequency of review. The level of insurance cover and any key exclusions or non-standard terms should be noted, including self-insurance in terms of the manager's approach and controls to ensure adequacy • Volume and types of insurance claims, historically and any outstanding	• Relative adequacy of insurance coverage is generally appropriate in comparison to other peers of a similar size, structure and complexity • Annual review cycle of insurance coverage

C.2 Personnel - corporate / enterprise

Personnel – corporate / enterprise

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

Scope	Examples of policy/documents	Examples of qualitative assessment and observation	Examples of good practice
Organisation, resourcing, and culture • Succession planning • Organisational chart • HR team structure • Turnover • Diversity, equity and inclusion • Leave and working arrangements	• Succession plans • Roles and responsibilities for employees • Diversity, Equity and Inclusion policy • Whistleblower policy • Bullying, discrimination and harassment policy • Code of Conduct/Ethics • Employee engagement surveys	• Formal succession planning process that is reviewed regularly. • Document equity succession planning procedures • An assessment of the capability and numbers of key staff in operational areas • Turnover of employees in investment and non-investment teams and causes of the turnover • What initiatives are in place to improve diversity, equity and inclusion within the workplace • Analysis of the employee engagement score and establishment of an action plan • Understanding the process for anonymous reporting, investigation and management of harassment, bullying, discrimination and/or workplace violence	• Documented functional succession plans for key executives and other employees which is reviewed on a periodic basis • Provisions in place for the firm to buy back equity from key stakeholders upon their departure from the business • Flexible working arrangements are formalised • Leave arrangements are formalised and require employees to take a minimum number of consecutive leave days every year • Formal Diversity and Inclusion policy, with programs and practices embedded within the organisation, with accountability for Diversity and Inclusion • A formal whistleblowing policy, with an external whistle blowing hotline and regular reporting to the board

Personnel – corporate / enterprise

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

Scope	Examples of policy/documents	Examples of qualitative assessment and observation	Examples of good practice
Remuneration and performance management • Compensation and incentive process • Long and short term incentives • Performance management	• Performance management policy	• Frequency of performance reviews and whether there is a formal process for objective setting, and review of objectives • Assessment of compensation and whether there is a process to benchmark with the industry • Assessment of the split between short term and long term incentives for executives, investment and non-investment teams • Assessment of any long term incentive and carry programs	• 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 • Employees are assessed against financial and non-financial objectives • Carried interest contributions should be on a whole fund basis
Training and development • Training for new and existing staff	• Training policy	• Assessment of mandatory training for new employees and for employees on an ongoing basis • Policies and programs in place to assist with the development of employees	• Additional development and learning opportunities available to staff to upskill, for example opportunities to attend conferences and pursue higher education (such as the CFA program). • Regular training on HR policies
Recruiting and background checks • Recruitment process • Background checks	• Recruitment policy	• Process for recruiting new employees • Background checks for new and existing employees	• Formal process for recruitment of employees • Comprehensive background checks prior to employment and on an ongoing basis (subject to legal jurisdiction)

C.3 Governance – corporate / enterprise

Governance – corporate / enterprise **Objective**: Assess the appropriateness of the governance, risk and compliance frameworks to drive effective decision making and to ensure that all associated risk and compliance practices are adequate with the relevant risks captured, monitored, and reported to management/committee/board levels appropriately to promote a proactive risk culture.			
Scope	**Examples of policy/documents**	**Examples of qualitative assessment and observation**	**Examples of good practice**
• Governance framework • Reporting lines	• Governance Frameworks/Policies	• The organisational structure reinforces effective oversight with an independent governing body and appropriate sub-committees • There are adequate processes and protocols in place to provide information to senior management and the governing body allowing them to make effective decisions • The organisational structure promotes clear segregation of duties between investment, operational, and control functions • Control departments (internal audit, risk control, and compliance) have reporting lines (direct and indirect) that can demonstrate independence from the business	• Maintenance and regular review of formal Governance Frameworks/Policies

Governance – corporate / enterprise

Objective: Assess the appropriateness of the governance, risk and compliance frameworks to drive effective decision making and to ensure that all associated risk and compliance practices are adequate with the relevant risks captured, monitored, and reported to management/committee/board levels appropriately to promote a proactive risk culture.

Scope	Examples of policy/documents	Examples of qualitative assessment and observation	Examples of good practice
• Board and Committee structures	• Terms Of Reference • Board Charters • Meeting minutes	• The governing body and committees have clearly defined and documented responsibilities, authorities, delegations, membership, and controls • Clear reporting structure from Management to Boards and Board Committees, ensuring clear segregation and independence	• Boards, Board Committees and Management Committees are governed by formal Charters and hold regular meetings, which have minutes • Boards and Board Committees include independent Directors with a diverse range of background and skillset. Good practice is to have independent representation on Boards and Board Committees • Demonstrable understanding of the differences between risk and compliance and appropriate practices for both • Regular review of policies
• Risk culture	• Risk Appetite Statement • Risk Management Framework (RMF) • Compliance Framework/Plan	• Alignment of corporate risk culture • Top down ownership and accountability of risk culture, and its level of permeation through the business, including support from senior management • Transparency demonstrated by the business in responding to operational due diligence • Assessment of the Risk Management Framework and its alignment to the industry enterprise risk frameworks	• Maintenance and regular review of a formal 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 • At a minimum, the RMF should address the following risks: operational, reputational, strategic, compliance, liquidity, investment, benchmark, capacity, geopolitical, offshoring and counterparty • Evidence of clear ownership and accountability of risk management, at the Board/Committee levels through proactive management of risk

Governance – corporate / enterprise

Objective: Assess the appropriateness of the governance, risk and compliance frameworks to drive effective decision making and to ensure that all associated risk and compliance practices are adequate with the relevant risks captured, monitored, and reported to management/committee/board levels appropriately to promote a proactive risk culture.

Scope	Examples of policy/documents	Examples of qualitative assessment and observation	Examples of good practice
			Management Framework and monitoring of risk registers • 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. Appropriately experienced compliance, risk and internal audit personnel. • The firm has been transparent and has provided an adequate amount of information • The firm has demonstrated a willingness to address any risk concerns raised in response to operational due diligence • Regular Risk Culture Surveys are conducted, and participation rates are indicative of a strong risk culture
• Risk Management	• Risk registers • Reporting to Boards/Committees	• Evidence of testing of risks, with formal reporting to Committee and Boards • Risk registers cover all key areas of operational risks and are regularly reviewed and updated	• Good practice is to have risk management as a standing agenda item and regular reporting at Board meetings • Risks are identified, assessed, and managed appropriately and on a timely basis. Regular review of risk related registers and assessment of risks within the business units and emerging risks • Regular Risk Culture Surveys are conducted, and participation rates are indicative of a strong risk culture • Identify any risks that the investment manager is not adequately acknowledging or addressing

Governance – corporate / enterprise

Objective: Assess the appropriateness of the governance, risk and compliance frameworks to drive effective decision making and to ensure that all associated risk and compliance practices are adequate with the relevant risks captured, monitored, and reported to management/committee/board levels appropriately to promote a proactive risk culture.

Scope	Examples of policy/documents	Examples of qualitative assessment and observation	Examples of good practice
	• Breaches and incidents policy and register	• Sighting breaches/incidents registers • Breaches and incident Policy includes details on how an incidents are determined, reported and managed (internal and external)	• Breaches/incidents are appropriately identified, managed and reported to the appropriate levels of management • A process is in place to ensure that incidents with recurring root causes are identified and rectified on a timely basis
Internal / External Audit	• Independent internal controls report (that is, GS007 or equivalent)	• Internal Controls Report (including IT equivalent) is performed by an appropriately qualified party • Review of approach for Internal Audit Plan	• 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 • A risk based approach is used to determine the Internal Audit Plan • Internal audit team reports directly to the Audit Committee • Independent internal control audit opinions are unqualified. Where issues have been identified in the independent internal controls report, management have an appropriate and timely remediation

Governance – corporate / enterprise

Objective: Assess the appropriateness of the governance, risk and compliance frameworks to drive effective decision making and to ensure that all associated risk and compliance practices are adequate with the relevant risks captured, monitored, and reported to management/committee/board levels appropriately to promote a proactive risk culture.

Scope	Examples of policy/documents	Examples of qualitative assessment and observation	Examples of good practice
• Compliance	• Compliance plan and frameworks • Reporting to Boards/Committees	• 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 • Assess the process on how the investment manager ensures they comply with relevant laws and regulations within its jurisdiction • Assess the process for identification, assessment and management of new regulatory changes • 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	• 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 Any compliance breaches are identified and managed on a timely basis • No regulatory breaches or license restrictions • Compliance frameworks and plans are reviewed and audited independently on a periodic basis • Consistent and robust process for identification and implementation of new or updated regulatory obligations in all of the jurisdiction which the Investment Manager operates in • Investment Manager has appropriate licences in the locations it operations in

Governance – corporate / enterprise

Objective: Assess the appropriateness of the governance, risk and compliance frameworks to drive effective decision making and to ensure that all associated risk and compliance practices are adequate with the relevant risks captured, monitored, and reported to management/committee/board levels appropriately to promote a proactive risk culture.

Scope	Examples of policy/documents	Examples of qualitative assessment and observation	Examples of good practice
Conflicts of Interest	• Conflicts of interest policy	• Conflicts of Interest Policy (including related party management) and details of how conflicts are mitigated, monitored, reported, and managed	• Conflicts of interests (including personal trades, gifts and entertainment) are appropriately identified, reported and managed
	• Personal Trading Policy • Gifts and Entertainment Policy • Conflicts of Interest • Material non-public information	• Personal trading and gifts and entertainment Policies include appropriate controls to ensure that conflicts of interest are appropriately identified, managed, reported, and mitigated • Gift and Hospitality Policy with a gift/benefit register and details including any limits and pre-clearances and what would cause a breach • Assess whether there are any potential or actual information barriers within the entity	• Personal trading policy includes a minimum holding period, management of restricted lists, and regular oversight of personal trades. Appropriate limits and aggregate limits are set for gifts and entertainment with approvals and oversight by the Compliance team

C.4 Trading processes and operational functions - listed asset classes and open ended pooled funds

Trading and back-office

To ensure the investment manager has appropriate trading policies and systems in place relative to the asset class, specifically addressing transparency, robustness, segregation of duties and effectiveness and is able to implement the strategy as it has been communicated. Assess the quality of existing reporting, its timeliness and compliance with regulatory requirements as appropriate

Scope	Examples of policy/documents	Examples of qualitative assessment and observation	Examples of good practice
• Best Execution and Counterparties	• Broker execution policy • Counterparty management policy • Currency / FX Policy	• Process for overseeing counterparties • ISDA agreements in place • Currency management processes documented and subject to trading controls	• Due diligence conducted on brokers prior to appointment and on a regular basis • Appropriate segregation between the dealers and the approval of brokers • A committee approves a broker to the panel. Formal review of the approved broker panel performed regularly • Evidence of multiple quotes being obtained for fixed income trades (to support best execution monitoring) or supporting commentary as to why multiple quotes weren't obtained • ISDA agreements with CSAs in place with counterparties. Key terms (such as, NAV floors and ATEs) of the ISDA agreements are subject to periodic review and broadly consistent, where possible • Formal counterparty risk monitoring and reporting

Trading and back-office

To ensure the investment manager has appropriate trading policies and systems in place relative to the asset class, specifically addressing transparency, robustness, segregation of duties and effectiveness and is able to implement the strategy as it has been communicated. Assess the quality of existing reporting, its timeliness and compliance with regulatory requirements as appropriate

Scope	Examples of policy/documents	Examples of qualitative assessment and observation	Examples of good practice
• Trading processes • Trade execution • Trade allocation • Trading systems used	• Trading and allocation policy • Cross trading policy • Soft dollar policy • Trade error policy • Derivatives Risk policy	• Segregation of roles and responsibilities between front office, middle office and back office • Independent Transaction Cost Analysis • Process for trade allocation • Process for trade cancelations • Processes that are manual vs systemised • Demonstration of independent oversight for cross trading and non-standard trading as well as related party engagement • Collateral management procedures • Derivative reporting processes	• Transactions are independent verified and there are appropriate processes to ensure transparency and role segregation • Formalised policies and procedures for key trading and operational processes • Appropriate segregation between order entry, trade execution, trade management and investment compliance • Evidence of review of trade allocation for fairness • Formal process for allocations, and non-standard allocations are overseen by a non investment team • Documented maker-checker reviews for manual processes

Trading and back-office

To ensure the investment manager has appropriate trading policies and systems in place relative to the asset class, specifically addressing transparency, robustness, segregation of duties and effectiveness and is able to implement the strategy as it has been communicated. Assess the quality of existing reporting, its timeliness and compliance with regulatory requirements as appropriate

Scope	Examples of policy/documents	Examples of qualitative assessment and observation	Examples of good practice
• Mandate Compliance	• Investment compliance policy	• Process for inputting guidelines (hard and soft) to the system • Percentage of manual vs systematised guidelines • Process for managing pre and post trade compliance alerts • Frequency of reconciling trade guidelines with the mandate • Process for managing trading and investment compliance breaches	• Guidelines are input by a team outside the investment team and subject to periodic review and sign off • Majority or all guidelines are within the system. • Investment team are prevented from overriding hard coded guidelines • Investment compliance team review and investigate post trade compliance breaches • Trading and investment compliance breaches are recorded and managed by the risk and compliance team. Mitigating actions are implemented to prevent re-occurrence • Clients and investors are made whole where the error has caused a negative impact. Any gains are retained • Regular reconciliation of rules to mandates
• Back office • Confirmation • Settlement • Reconciliation		• Process for communicating trades to the custodian • Cash management processes and controls • Processes that are manual vs systemised • Process and frequency of reconciliations	• Cash and stock reconciliations are performed on a daily basis (or commensurate with the liquidity of the portfolio) with exceptions investigated and rectified on a timely basis • there is a four-eye check process for reconciliations • Appropriate delegations

Trading and back-office

To ensure the investment manager has appropriate trading policies and systems in place relative to the asset class, specifically addressing transparency, robustness, segregation of duties and effectiveness and is able to implement the strategy as it has been communicated. Assess the quality of existing reporting, its timeliness and compliance with regulatory requirements as appropriate

Scope	Examples of policy/documents	Examples of qualitative assessment and observation	Examples of good practice
Proxy voting and Class Actions	• Proxy Voting Policy • Class Actions	• Review the Class Action and proxy Policy and details of the investment manager's default position in the absence of instructions from the asset owner • Provision of class action data and recommendations (subject to mandate)	• Challenge and discussion within the manager prior to voting against provider policies • Reconciliation of votes vs direction of client (pooled) where possible • Engagement with underlying assets (where requested in the mandate)
Reporting	• Policies / process materials documenting reporting requirements by client / type • Proxy reporting • Regulatory and breach reporting	• Differences between mandate / unlisted reports and breaches • Automatic generation of reports	• Clear reports delivered via portal • Oversight and review, independent of the investment function • Reporting system automated with limited manual intervention • Reports process audited by an independent party

C.5 Trading processes and operational functions – real asset classes and closed end funds

Trading and back-office

To ensure the investment manager has appropriate trading policies and systems in place relative to the asset class, specifically addressing transparency, robustness, segregation of duties and effectiveness and is able to implement the strategy as it has been communicated. Assess the quality of existing reporting, its timeliness and compliance with regulatory requirements as appropriate

This section may need to be adjusted by the reviewer to appropriately review the specific strategy (real assets won't have counterparties, some unlisted assets / closed assets will).

Scope	Examples of policy/documents	Examples of qualitative assessment and observation	Examples of good practice
• Best Execution and Counterparties	• Broker execution policy • Counterparty management policy • Currency / FX Policy	• Process for overseeing counterparties • ISDA agreements in place • Currency management processes documented and subject to trading controls	• Due diligence conducted on brokers prior to appointment and on a regular basis • Appropriate segregation between the dealers and the approval of brokers • A committee approves a broker to the panel. Formal review of the approved broker panel performed regularly • Evidence of multiple quotes being obtained for fixed income trades (to support best execution monitoring) or supporting commentary as to why multiple quotes weren't obtained • ISDA agreements with CSAs in place with counterparties. Key terms (such as, NAV floors and ATEs) of the ISDA agreements are subject to periodic review and broadly consistent, where possible • Formal counterparty risk monitoring and reporting

Trading and back-office

To ensure the investment manager has appropriate trading policies and systems in place relative to the asset class, specifically addressing transparency, robustness, segregation of duties and effectiveness and is able to implement the strategy as it has been communicated. Assess the quality of existing reporting, its timeliness and compliance with regulatory requirements as appropriate

This section may need to be adjusted by the reviewer to appropriately review the specific strategy (real assets won't have counterparties, some unlisted assets / closed assets will).

Scope	Examples of policy/documents	Examples of qualitative assessment and observation	Examples of good practice
• Deal processes • Deal execution • Deal allocation • Systems / models used	• Deal allocation policy • Cross trading policy • Trade error policy • Derivatives Risk policy	• Segregation of roles and responsibilities between front office, middle office and back office • Process for deal allocation • Processes that are manual vs systemised • Demonstration of independent oversight for cross trading and non-standard trading as well as related party engagement • Collateral management procedures • Derivative reporting processes	• Transactions are independent verified and there are appropriate processes to ensure transparency and role segregation • Formalised policies and procedures for key dealing and operational processes • Appropriate segregation of duties • Evidence of review of trade allocation for fairness • Formal process for allocations, and non-standard allocations are overseen by a non investment team • Documented maker-checker reviews for manual processes • Robust cross trade management with non-investment oversight

Trading and back-office

To ensure the investment manager has appropriate trading policies and systems in place relative to the asset class, specifically addressing transparency, robustness, segregation of duties and effectiveness and is able to implement the strategy as it has been communicated. Assess the quality of existing reporting, its timeliness and compliance with regulatory requirements as appropriate

This section may need to be adjusted by the reviewer to appropriately review the specific strategy (real assets won't have counterparties, some unlisted assets / closed assets will).

Scope	Examples of policy/documents	Examples of qualitative assessment and observation	Examples of good practice
• Fund / Vehicle Compliance	• Investment compliance policy	• Process for inputting guidelines (hard and soft) to the system and appropriate oversight of whole of fund limits. • Percentage of manual vs systematised guidelines • Process for managing investment compliance breaches	• Guidelines are input by a team outside the investment team and subject to periodic review and sign off • Majority or all guidelines are within the system • Investment team are prevented from overriding hard coded guidelines • Investment compliance team review and investigate post trade compliance breaches • Trading and investment compliance breaches are recorded and managed by the risk and compliance team. Mitigating actions are implemented to prevent re-occurrence • Clients and investors are made whole where the error has caused a negative impact. Any gains are retained • Regular reconciliation of rules to mandates

Trading and back-office

To ensure the investment manager has appropriate trading policies and systems in place relative to the asset class, specifically addressing transparency, robustness, segregation of duties and effectiveness and is able to implement the strategy as it has been communicated. Assess the quality of existing reporting, its timeliness and compliance with regulatory requirements as appropriate

This section may need to be adjusted by the reviewer to appropriately review the specific strategy (real assets won't have counterparties, some unlisted assets / closed assets will).

Scope	Examples of policy/documents	Examples of qualitative assessment and observation	Examples of good practice
• Back office • Confirmation • Settlement • Reconciliation		• Process for communicating trades to the custodian / administrator (as appropriate) • Cash management processes and controls • Processes that are manual vs systemised. • Process and frequency of reconciliations	• Reconciliations are performed on a daily basis (or commensurate with the liquidity of the portfolio) with exceptions investigated and rectified on a timely basis • There is a four-eye check process for reconciliations • Appropriate delegations have been set up
Proxy voting and Class Actions (Fund, may not apply for closed end / real assets)	• Proxy Voting Policy • Class Actions	• Review the Class Action and proxy Policy and details of the investment manager's default position in the absence of instructions from the asset owner • Provision of class action data and recommendations (subject to mandate)	• Challenge and discussion within the manager prior to voting against provider policies • Reconciliation of votes vs direction of client (pooled) where possible • Engagement with underlying assets (where requested in the mandate)

Trading and back-office

To ensure the investment manager has appropriate trading policies and systems in place relative to the asset class, specifically addressing transparency, robustness, segregation of duties and effectiveness and is able to implement the strategy as it has been communicated. Assess the quality of existing reporting, its timeliness and compliance with regulatory requirements as appropriate

This section may need to be adjusted by the reviewer to appropriately review the specific strategy (real assets won't have counterparties, some unlisted assets / closed assets will).

Scope	Examples of policy/documents	Examples of qualitative assessment and observation	Examples of good practice
Reporting	• Policies / process materials documenting reporting requirements by client / type • Proxy reporting • Regulatory and breach reporting	• Automatic generation of reports	• Clear reports delivered via portal • Oversight and review, independent of the investment function • Reporting system automated with limited manual intervention • Reports process audited by an independent party

C.6 Valuations - listed

Valuations – listed

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 liquid markets.

Scope	Examples of policy/documents	Examples of qualitative assessment and observation	Examples of good practice
Governance	Valuation Committee terms of reference / charter	• process for managing valuations (such as approval, rejection, and reassessment) • pricing of securities • triggers for out-of-cycle valuations • Ability for exceptions and overrides • management of stale prices • valuation committee structure and internal governance to address complex valuation issues	• Non-conflicted committee • Independent experts • Regular meetings, documented • Clear roles and responsibilities • independent pricing of securities • Periodic revision of policy and oversight of process • Register of non standard prices / exceptions to process • Clear escalation and resolution procedures
Inputs (may be asset class / instrument specific)	Listed valuation policy	• Definitions of level 1, 2 and 3 assets • Pricing hierarchy for vendors • Processes for stale and suspended assets	• Alignment with industry standards • Clear documentation of Level 1, 2, 3 assets • Periodic revision • Consistent methodology
Cryptocurrency and digital assets	Policy	• Confirm whether crypto and digital assets are held within the portfolio. Clearly document in report outcomes	

Valuations – listed

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 liquid markets.

Scope	Examples of policy/documents	Examples of qualitative assessment and observation	Examples of good practice
Methodologies (assumptions, timing and frequency)	Methodology documentation	• Assumptions documentation • Frequency of valuations	• Controls testing (internal and external) • Clearly articulated and documented methodology and escalation to Committee for methodology change • Input validity testing
Team completing (insourced / outsourced)	Documented roles and responsibilities	• Experiences of employees involved in the valuation process.	• Appropriately qualified team • Independent, segregation of duties between investments and valuer • If outsourced, rotation of valuer / team
Oversight	Documented roles and responsibilities	• Responsibility of oversight roles • Trigger and escalation documentation available. Process for escalations • Board and risk reporting	• Review by independent audit or alternative party • Regular reporting to the Board / Risk Committee as appropriate • Appropriate delegations for approving amendments to valuations • Documentation of exemptions and stale valuations etc
Audit		• Independent verification of valuation assumptions • Confirmation of appropriate implementation	

C.7 Valuations – all

Valuations – all **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 unlisted and illiquid markets.			
Scope	**Examples of policy/documents**	**Examples of qualitative assessment and observation**	**Examples of good practice**
Governance	Valuation Committee terms of reference / charter	• process for managing valuations (such as approval, rejection, and reassessment) • pricing of securities • triggers for out-of-cycle valuations • Ability for exceptions and overrides • management of stale valuations • valuation committee structure and internal governance to address complex valuation issues	• Non-conflicted committee • Independent experts, including periodic review / review of valuers • Regular meetings, documented • Clear roles and responsibilities • independent pricing of assets • Periodic revision of process and Policy • Clear escalation and resolution procedures
Inputs (may be asset class / instrument specific)	Listed valuation policy Unlisted valuation policy	• Definitions of level 1, 2 and 3 assets	• Alignment with industry standards by sector, such as IPEV (International Private Equity Valuations), Fair Market Value etc • Clear documentation of Level 1, 2, 3 assets. • Periodic revision • Oversight by audit
Cryptocurrency and digital assets	Policy	• Confirm whether crypto and digital assets are held within the portfolio. Clearly document in report outcomes	

Valuations – all

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 unlisted and illiquid markets.

Scope	Examples of policy/documents	Examples of qualitative assessment and observation	Examples of good practice
Methodologies (assumptions, timing and frequency)	Methodology documentation	• Assumptions documentation • Roles and responsibility for methodology changes • Frequency of valuations	• Controls testing (internal and external) • Clearly articulated and documented methodology and escalation to Committee for methodology change • Input validity testing • Documentation of exemptions and out of cycle valuations, stale valuations etc • Quarterly valuations for private market assets • Evidence of back testing
Team completing (insourced / outsourced)	Documented roles and responsibilities	• Experiences of employees involved in the valuation process	• Appropriately qualified team • Independent , segregation of duties between investments and valuer • If outsourced, rotation of valuer / team • Independent verification of valuation assumptions

Valuations – all

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 unlisted and illiquid markets.

Scope	Examples of policy/documents	Examples of qualitative assessment and observation	Examples of good practice
Oversight	Documented roles and responsibilities	• Responsibility of oversight roles • Trigger and escalation documentation available. Process for escalations • Board and risk reporting	• Review by independent audit or alternative party • Quantitative triggers to prompt more frequent valuations, including in times of distress • Appropriate sign off by Valuation Committee under recognised delegations and appropriate governance • Regular reporting to the Board / Committee as appropriate • Appropriate delegations for approving amendments to valuations and / or methodology • Documentation of any exemptions
Audit		• Independent verification of valuation assumptions	

C.8 IT systems and security - enterprise

IT systems and security - enterprise **Objective**: To ensure the investment manager's IT systems and security processes are appropriate for the asset class, region (including to regulatory standards impacting certain Australian investors – for example, CPS 234, CPS 230, etc) 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. Consider the ability and intent of the manager to ensure future data and technology security.			
Scope	**Examples of policy/documents**	**Examples of qualitative assessment and observation**	**Examples of good practice**
IT Governance	Internal controls and IT audit Risk findings related to IT	• Regular discussion of IT at the risk committees and Board • Oversight of IT outcomes and review of regular improvements • Review of roles and responsibilities for appropriateness	• Independent assurance over IT framework • ISO27001 certification and / or evidence of assurance over NIST alignment • Ongoing training for Board and staff • Maintains a register of critical models and spreadsheets. The register of critical models and or spreadsheets is regularly reviewed and assessed for relevant risks • Appropriate Reporting to Board and Risk Committees, standing item in meetings

IT systems and security - enterprise

Objective: To ensure the investment manager's IT systems and security processes are appropriate for the asset class, region (including to regulatory standards impacting certain Australian investors – for example, CPS 234, CPS 230, etc) 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. Consider the ability and intent of the manager to ensure future data and technology security.

Scope	Examples of policy/documents	Examples of qualitative assessment and observation	Examples of good practice
IT infrastructure / architecture and resourcing	• Procedure manuals for proprietary applications • Network and systems diagrams • Audits for proprietary systems • Documented roles and responsibilities	• Is the IT infrastructure and resourcing commensurate with the size of the business and the asset class being managed? • Are there any key person risk in relation to proprietary applications? • Where the IT function is outsourced, who is responsible for the management of the relationship and does the individual appear to have an appropriate level of understanding of the firm's IT environment? • Appropriate oversight and accountability for the IT and cybersecurity environment from a governance function • Understanding and oversight of third party applications that have access to the network	• Where the firm utilises a private cloud environment, it has appropriate protections in place to ensure retention of its own data/IP • Formalised upgrade/update programs for infrastructure, hardware, and applications (for example, patch management) • Administration rights limited for the network and any firm-issued hardware • Processes in place to monitor the hardware redundancy and capacity levels to ensure sufficient resources

IT systems and security - enterprise

Objective: To ensure the investment manager's IT systems and security processes are appropriate for the asset class, region (including to regulatory standards impacting certain Australian investors – for example, CPS 234, CPS 230, etc) 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. Consider the ability and intent of the manager to ensure future data and technology security.

Scope	Examples of policy/documents	Examples of qualitative assessment and observation	Examples of good practice
Cybersecurity controls and testing	• Cybersecurity policy • Incident response plan • Acceptable use policy	• Does the suite of cybersecurity policies capture key cybersecurity considerations (for example, incident management procedures, firewalls, anti-virus and malware, data encryption, password rules, remote access, mobile devices, patch management, testing and vulnerability assessments, etc) • SOC/SIEM and ongoing network monitoring processes, including triage and escalation procedures • Is multi-factor authentication utilised where enabled to do so • The firm has a policy of notifying investors in the event of a data breach, even if no client data was stolen	• Independent penetration (external and internal) testing / cloud configuration reviews, with periodic rotation of testers • Ongoing vulnerability scanning • Independent assurance of alignment to recognised industry frameworks (such as NIST, ISO 27001, Essential Eight) • Testing/training for the key members of the incident response plan • Cyber awareness training (including phishing) for all staff • Use of password management tools • Policies or procedures (that is, regular, formal monitoring) in place to ensure third parties with access to the network have appropriate cybersecurity controls • Building, office, and data centre locations are physically secure • Regular phishing testing

IT systems and security - enterprise

Objective: To ensure the investment manager's IT systems and security processes are appropriate for the asset class, region (including to regulatory standards impacting certain Australian investors – for example, CPS 234, CPS 230, etc) 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. Consider the ability and intent of the manager to ensure future data and technology security.

Scope	Examples of policy/documents	Examples of qualitative assessment and observation	Examples of good practice
Data security controls	• Information security policy • Acceptable use policy • Privacy policy • Data quality and governance policy • Role based access control (RBAC) Guidelines	• Does the firm employ data classification protocols and are there additional controls applied when transmitting sensitive or confidential data • Are SFTP and/or secure platforms used for communications? • Systematised RBAC	• Data loss prevention tools • RBAC which are subject to regular review and sign off, as well as audit • Endpoint controls • Mobile device management protocols • Default use of encryption and password protection when transmitting sensitive or PII data via email • Portable storage devices may be prevented • 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
Change management policy and related procedures	• Change management policy	• There are controls and processes around system and model development	• Appropriate segregation and controls surrounding application deployment to limit unauthorised changes to the production environment • Changes are authorised, monitored, tested and approved prior to implementation • Controls are reaffirmed, including access controls for internal and third-party users

IT systems and security - enterprise

Objective: To ensure the investment manager's IT systems and security processes are appropriate for the asset class, region (including to regulatory standards impacting certain Australian investors – for example, CPS 234, CPS 230, etc) 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. Consider the ability and intent of the manager to ensure future data and technology security.

Scope	Examples of policy/documents	Examples of qualitative assessment and observation	Examples of good practice
AI (Artificial Intelligence)	• AI usage policy • Acceptable use policy	• Is there a governance framework in place to oversee the use of generative AI and who is tasked with oversight of AI usage • Does the policy covering AI address ethical considerations, regulatory compliance, and risk management • What controls in place to protect sensitive and/or confidential data used in generative AI applications • Where a third party AI tool is being utilised (such as Microsoft 365 Copilot. How does the firm ensure segregation of internal data from public access • Has the firm sought to address data ownership and privacy considerations/regulations	• Training programs for staff in relation to the use of AI • AI usage and associated risks are incorporated into the firm's risk management framework and/or compliance monitoring processes • Restricting access and use of publicly available AI website whilst connected the network • AI-specific threats and risks have been incorporated into the firm's cybersecurity program (for example, awareness training and cyber-risk considerations)
Spreadsheet controls	• Model and Spreadsheet management policy	• Where the firm uses spreadsheets, are there appropriate controls utilised (locked cells, macros, restricted access, etc)	• Periodic version control audits and back testing • Maker-checker processes • Independent assurance, particularly in relation to models used as inputs to decision making

C.9 Business continuity

Business continuity **Objective**: To assess the investment manager's BCP and DRP and be assured that it is appropriately tested and maintained.			
Scope	**Examples of policy/documents**	**Examples of qualitative assessment and observation**	**Examples of good practice**
Business continuity • Scenarios • Recovery strategies • Business impact analysis • Crisis team	• Business Continuity Management Policy (BCMP) • Business Continuity Plan BCP) • Test results	• Frequency of review and testing, process to manage findings and improvement opportunities identified • Inclusion of service providers in its BCP testing • How are critical staff determined. • Training for employees • Scenarios included in the BCP • Management of actual BCP events • Outcome from the most recent test	• BCMP is reviewed at least annually by a governing body. BCMP includes critical business activities, recovery objectives, key roles and responsibilities, and response plans to plausible disruption scenarios • Dedicated crisis management team (CMT) is in place and undergoes regular training and testing • Issues and areas of opportunities are identified, recorded and managed until completion • Oversight by the Risk Committee and Board. • Employees are provided training on a regular basis • BCP and testing cover various scenarios (for example, not just working from home) • Critical service providers are included in the BCP testing, or the investment manager has been included in the service provider's BCP test
Disaster recovery	• Disaster recovery plan • Test results	• Frequency of review and testing, process to manage issues and improvement opportunities identified • Extent of the failover testing • How are critical systems identified • Outcome from most recent DR test	• DRP is reviewed at least annually • Full failover testing is completed annually with partial failover testing completed throughout the year • Issues and areas of opportunities are identified, recorded and managed until completion • Oversight by the Risk Committee and Board

Business continuity **Objective**: To assess the investment manager's BCP and DRP and be assured that it is appropriately tested and maintained.			
Scope	**Examples of policy/documents**	**Examples of qualitative assessment and observation**	**Examples of good practice**
Call tree testing		• Frequency of call tree testing • Process for capturing and updating employee details • System and process used to enact the call tree	• Call tree testing undertaken at least annually • Call tree testing is managed within a system which is connected to the Human Resources system to ensure that employee details are updated on a real time basis

C.10 Service provider oversight

Service Provider Oversight

Objective: Assess the extent to which the investment manager has material service providers (including any related parties) and that these are adequately documented and managed. Examples of material outsourced arrangement may include Custody, IT, Middle Office, Fund Administration, Prime Brokerage, and Unit Registry.
This should be applied equally to third party and related party service providers.

Scope	Examples of policy/documents	Examples of qualitative assessment and observation	Examples of good practice
New service providers • Due diligence process	• Vendor management policy • Outsourcing policy • Service Level Agreements (SLA) • Derivatives Policy • Modern slavery policy • Supplier Code of Conduct	• What is the process the investment manager has undertaken to identify whether the service provider was fit for purpose • Due diligence process undertaken for selecting and appointing a service provider • Due diligence process undertaken for related party providers	• A formal service provider policy maintained are regularly reviewed, which includes contingency plans and exit strategies • Relevant stakeholders are included in the due diligence process including risk, compliance and IT • Formal RFP process for critical/key service providers

Existing service providers
• Ongoing monitoring
• Due diligence process
• Benchmarking process
	• Service provider performance report
	• Vendor management policy
	• Outsourcing policy
		• Oversight process that is undertaken for existing service providers and related parties – that is, frequency that
		  ○ the service provider's performance is reviewed
		  ○ a benchmarking review is conducted
		  ○ full due diligence is undertaken
		• Reporting that is provided to relevant committees and boards on material service providers
			• 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)
			• Annual onsite due diligence of key third parties and should include periodic onsite reviews of locations performing the services
			• External benchmarking reviews undertaken periodically for all material service providers including related parties

C.11 Environmental, social & corporate governance – enterprise

Environmental, social & corporate governance - enterprise

Objective: To assess the sustainability and social impact of the investment manager's corporate operations and controls (including to regulatory standards impacting certain Australian investors – for example, CPG 229, etc).

Scope	Examples of policy/documents	Examples of qualitative assessment and observation	Examples of good practice
Governance and oversight of the Corporate ESG program	• ESG policy • Responsible investment policy • Modern slavery statements • ESG Incident Log	• Regular oversight by a senior governing body, including reviewing relevant reporting • How does a firm seek to implement the 'social' aspects of its ESG framework, both internally (health and safety, modern slavery, supply chain management, etc) and within the wider community (such as outreach programmes, volunteering days, charitable donations, etc)	• ESG policies and procedures are reviewed and updated regularly and reflect changes in regulation and contemporary ESG practices • ESG policies include detail on internal reporting and escalation processes • ESG should be a standing agenda item of the firm's principal governance function or underlying committee, with appropriate reporting and escalation procedures, as needed • ESG awareness training, to ensure employees remain abreast of a firm's ESG policies and principles • Demonstrable logs of ESG incidents and anticipated resolutions / awareness
Climate change risk	• Task Force on Climate-related Financial Disclosures (TCFD) reporting	• Has the firm set any corporate-ESG goals (such as carbon-neutrality, reduction in plastic waste, etc) and is their progress being monitored and reported externally • Is the firm specifically addressing climate change risks and opportunities, at a corporate-level • Is the firm captured by any regional regulatory requirements pertaining to climate change/risk.	• There are management systems and procedures for identifying, managing and reporting on the financial risks arising from climate change • Reporting is aligned to the TCFD

Environmental, social & corporate governance - enterprise **Objective**: To assess the sustainability and social impact of the investment manager's corporate operations and controls (including to regulatory standards impacting certain Australian investors – for example, CPG 229, etc).			
Scope	**Examples of policy/documents**	**Examples of qualitative assessment and observation**	**Examples of good practice**
		If so, do they apply a consistent approach across all jurisdictions?	
Monitoring of regulations and reporting	• Compliance monitoring program • Risk management framework • UNPRI report	• A control function monitors adherence to ESG-related regulations and reporting as part of its compliance monitoring program that includes regular testing • Where a firm subscribes to (or aligns with) ESG disclosure reporting standards (such as UNPRI, IRIS, TCFD, etc) or other initiatives (Transition Pathway Initiative, 30% Club, etc), who is responsible for reporting/monitoring adherence with the standard(s)/initiatives • Where a firm provides external corporate ESG reporting to an ESG reporting standards entity (such as UNPRI), there should be appropriate checks (by a control function) to ensure alignment with the standards, prior to publication	• Corporate - ESG risks are captured as part of a firm's ongoing compliance monitoring and risk management processes • ESG regulatory guideline monitoring and reporting is performed by an independent control function or by dedicated ESG resourcing, following the same incidents and breaches processes as any other regulatory guidelines
Investment application and recording of ESG factors	• Offering documents • Proxy voting policy • Responsible investment policy	• The firm actively considers ESG factors and their impact on investment decisions. These considerations are documented	• The firm's investment process incorporates ESG screening and/or ranking procedures, in addition to typical negative screening, into

Environmental, social & corporate governance - enterprise **Objective**: To assess the sustainability and social impact of the investment manager's corporate operations and controls (including to regulatory standards impacting certain Australian investors – for example, CPG 229, etc).			
Scope	**Examples of policy/documents**	**Examples of qualitative assessment and observation**	**Examples of good practice**
		• Systems and controls that allow a firm to evaluate underlying data that is used for ESG analysis and reporting, including quantifying the positive and negative impacts of its investing activities based on ESG factors • Does the firm engage in asset stewardship with portfolio companies to address and improve ESG-related issues, including documentation of any associated remedial actions	investment restrictions within fund offering documentation and SMA agreements • ESG investment guidelines/restrictions should be coded into the OMS, where possible. Where there is not possible, there should be suitable controls and reporting around manual guideline checks
Monitoring of regulations, reporting, and guidelines/restrictions	• Compliance monitoring program • Risk management framework • ESG Incident Log • UNPRI report	• A control function monitors adherence to ESG-related regulations, reporting and investor guidelines and restrictions as part of its compliance monitoring program that includes regular testing • Where a firm provides external ESG reporting to an ESG reporting standards entity (such as UNPRI), there should be appropriate checks (by a control function) to ensure alignment with the standards, prior to publication	• Investment-related ESG risks are captured as part of a firm's ongoing compliance monitoring and risk management processes • ESG regulatory guideline monitoring and reporting is performed by an independent control function or by dedicated ESG resourcing, following the same incidents and breaches processes as any other regulatory guidelines • Evidence of ESG Log if Manager is conducting ESG discussions on behalf of clients

D. Appendix 1 - Additional information for managers identified as material under CPS 230

Where an Investment Manager has been identified by a RSE as a material service provider under CPS 230, the below is intended to serve as a guide for additional operational due diligence discussion and reporting by the appointed third party/investment manager.

Importantly, the RSE / asset owner should discuss and agree with the Investment manager which of the RSEs' critical operations under CPS 230 are performed by the Investment Manager , noting that it will likely not be all services and processes performed by the Investment manager.

In considering the application of the below, ASFA encourages the operational due diligence reviewers to consider that while there is preferred documentation, consideration should be given to the care, skill and diligence of the investment manager, and thought to the potential for alternative supporting documentation if needed. to support the CPS 230 needs of the client. As noted above, while an Investment Manager may be noted as a material service provider by one RSE, it may not be considered material by another RSE. ASFA recognises that the Investment Manager may choose to provide additional CPS 230 confirmation / review to only the client that has identified it as material, or to all clients, at the Investment Manager's discretion.

In summary, RSEs should, before appointment and during the term of appointment:

- Affirm and periodically reaffirm that the manager / investment strategy and associated critical operations are / continue to be captured by CPS 230.
- Communicate and agree this with the Investment Manager
- Mutually agree with the Investment Manager what documentation will be made available during CPS 230 reviews
- Recognise the potential for CPS 230 requirements to cross over with other APRA Prudential Standards, such as CPS 234 *Information Security*, and others with clear intent to avoid duplication of process and request of information.
- The Investment Manager should, prior to engaging the operational due diligence reviewer and on an ongoing basis:
    - Confirm which of its processes have been identified as critical operations by the manager (to the client) captured by CPS 230
    - Agree these processes with clients that have designated the Investment Manager as captured under CPS 230

CPS 230 – Operational Risk Management

Objective: To assess operational risk management and resiliency as it pertains to RSE critical operations performed by a material service provider/investment manager. Much of the below is also covered in the Guidance above. The reviewer should consider any evidence and outcomes required to satisfy a critical operation completed by a material provider.

Scope	Examples of policy/documents	Examples of qualitative assessment and observation	Examples of good practice
Critical Operations Mapping	• Process maps where relevant	• Clearly mapped / documented internal processes linked to people, systems, locations	• Demonstration of Board oversight of critical operations

Operational Risk Management Framework (ORFM)	• Risk identification documents
	• Documented risk assessments, controls and monitoring
	• Incident and near miss protocols and registers
	• Offshoring and geographical risk
		• Operational model assessment
		  ○ Insource vs outsource
		  ○ Geographical location
		  ○ Geopolitical risk
		  ○ Data management
			• Broad integration with governance and assurance processes

Service Provider Risk Management	• Outsourcing / Procurement Policy ○ Exit Strategy and Transition Planning	• Pre appointment and ongoing monitoring of outsource providers and related parties • SLAs • KPIs • Periodic arm's length review • Clear path to transition outsource services with minimal / no impact on data portability and maintenance of service levels	• Integrated Board oversight of Outsourcing policy and practice • Strong management of related party outsourcing

CPS 230 – Operational Risk Management

Objective: To assess operational risk management and resiliency as it pertains to RSE critical operations performed by a material service provider/investment manager. Much of the below is also covered in the Guidance above. The reviewer should consider any evidence and outcomes required to satisfy a critical operation completed by a material provider.

Scope	Examples of policy/documents	Examples of qualitative assessment and observation	Examples of good practice
Business Continuity and Scenario Testing	• BCP Plan including documented scenarios • BCP Testing outcomes and remediations evidence • The above should include the processes / services mutually identified as critical		• Broad and consistent BCP planning and testing • Regular uplift • Integration of service providers into BCP testing
Resilience Metrics and Reporting	• Board papers displaying operational resilience oversight, including data issues or SLA breaches • Risk registers / logs including incidents / near misses, discussion of remediation		• Regular review and oversight by Board of Risk and Resiliency including KPIs and SLAs • Board consideration of outsource providers' resiliency, risk and incidents

CPS 230 – Operational Risk Management

Objective: To assess operational risk management and resiliency as it pertains to RSE critical operations performed by a material service provider/investment manager. Much of the below is also covered in the Guidance above. The reviewer should consider any evidence and outcomes required to satisfy a critical operation completed by a material provider.

Scope	Examples of policy/documents	Examples of qualitative assessment and observation	Examples of good practice
Information Security and Cyber Resilience	• Internal Controls / Audit for IT and Cyber processes if available • Evidence / discussion of alignment with NIST / ISO 27001, ASD Essential 8 as relevant • Evidence of cyber insurance • Penetration test results	• Appropriate access controls and relevant IT requirements such as patching, test environments etc.	• Regular review/uplift of IT and Cyber requirements
Data Governance and Privacy	• Data Governance Policy (including location management and data segregation) • Cloud Usage policy • AI Usage Policy	• Consideration given to location of data management as well as privacy laws	• Appropriate data management, archive, cloud and AI practices
Board Level Governance		• Regular consideration of operational risk and resiliency at the Board	• Demonstration of senior leadership accountability