FSC Guidance Note No. 52

Fund Manager Due Diligence (including CPS 230) Questionnaire

17 September 2024

FSC FINANCIAL SERVICES COUNCIL

FSC Guidance Note No.52

Fund Manager Due Diligence (including CPS 230) Questionnaire

Date of this version:	This version commenced on 17 September 2024. There are no previous versions.
Application of this Guidance Note:	This Guidance Note should be applied by fund managers in determining what documents and assurances to provide to superannuation funds seeking to comply with *APRA Prudential Standard CPS 230: Operational Due Diligence*.
Main Purpose of this Guidance Note:	The purpose of this Guidance Note is to provide a standardised due diligence framework for assessing a fund manager's suitability as a material service provider to a superannuation fund, under CPS 230.

FSC Guidance Note No. 52

Table of Contents

FSC Guidance Note No. 52

1. How to use this guidance

This questionnaire has been developed to assist superannuation funds in their approach to due diligence of funds management organisations as material service providers for the purposes of CPS 230: Operational Risk Management.

This questionnaire is not designed to represent a best practice approach to due diligence or compliance with CPS 230, but instead is designed as a menu of questions a superannuation fund may ask in their individualised approach to compliance with the Standard.

Superannuation funds may choose to use as many or as few questions as suits their needs with reference to the materiality of the services being provided to the individual superannuation fund, their risk appetite, and other individual circumstances. Superannuation funds may also ask additional questions, outside what is contained in this questionnaire.

Additionally, some of the information requested in this questionnaire may be supplied to the entity through the Investment Management Agreement Due Diligence or Request for Proposal processes, and as such, the superannuation fund may already have access to this information.

Use of and deviation from this questionnaire does not speak in any way to compliance with CPS 230 and is intended as a guide only.

2. Scope

The questions in this questionnaire, unless otherwise specified, relate specifically to the critical operations listed in the table in the Summary and the specific entity or mandate which is providing those services.

3. Definitions

Critical Operation means the operation or service as defined by the table at 4.1 which is provided by an entity to a superannuation fund. This critical operation or service has been determined by the superannuation fund to be critical to its operations under the Standard CPS 230: Operational Risk Management, meaning that a disruption beyond tolerance levels would have a material adverse impact on its customers, or its role in the financial system. The critical operations listed in this document should be those agreed by the superannuation fund and relevant organisation.

Material Service Provider(s) means the providers organisations relies on to undertake the critical operations listed in the table at 4.1 or that otherwise expose it to material operational risks that would risk the ability to provide the agreed critical operations listed at 4.1.

Relevant Organisation means the organisation relevant to the provision of the specific critical operation(s) or service(s). This may be the global or local entity, branch or division. Superannuation funds should agree with the relevant fund manager for which entity information is required.

Tolerance Levels tolerance levels are the agreed timeframe for an outage, after which any further outage would have a material adverse impact on its customers, or its role in the financial system. Tolerance levels include:

- The maximum period of time the superannuation fund would tolerate a disruption to the operation
- The maximum extent of data loss the superannuation fund would accept as a result of a disruption; and
- The minimum service levels the entity would maintain while operating under alternative arrangements during a disruption.

4. Summary

4.1 Agreed critical operations

Before completing this survey, the superannuation fund should complete the below table with the list of critical operations/services provided and the associated agreed tolerance levels. The questions in this document primarily pertain to the critical operations/services outlined in this table, and the entity providing the service.

FSC Guidance Note No. 52

Name of Critical Operation/Service	Description of Critical Operation/Service	Agreed Tolerance Level (specify days/hours etc)	Entity Providing Service*

* only complete this column if different businesses within the same entity are completing different operations (for example an Australian division versus the global entity).

Entity name(s) (list any entities responsible for the provision of the services listed above):
Address:
Contact details for respondent: Name of primary contact: Telephone: Email:
Relevant office locations, and functions performed in each geographical location:

5. Risk Management Framework

5.1 Operational Risk

5.1.1 Please provide a brief overview of your Risk Management Framework (as relevant to the business providing the critical operations listed in the Summary), including identifying and monitoring risk events, agreeing the mitigating actions and reporting to senior management.

5.1.2 Please provide a summary describing control and assurance activities that are performed in line with the framework to support the effectiveness of risk management activities and any material findings, as relevant to the provision of the critical operations listed in the summary and the business providing those services.

5.1.3 In addition to any control audit, please outline the process in place to monitor internal controls and application of procedures, as relevant to the provision of the critical operations listed in the summary and the business providing those services.

5.1.4 Does your organisation have a risk register in place? How is the risk register monitored and approved? Who is responsible for its maintenance?

5.1.5 Are there any specific political, economic, or geographical risks associated with the physical location of the relevant organisation's offices. If so, please explain how these are mitigated.

5.1.6 Do you have a risk acceptance process, relevant to the provision of the critical operations listed in the Summary, and do accepted risks require annual review?

5.1.7 Please provide a high-level overview of how external incidents and events are identified and assessed for any potential impacts on your business and explain how you adjust your control environment for these.

FSC Guidance Note No. 52

5.2 Critical Processes

5.2.1 Please provide a list of key business operations as it pertains to the provision of the critical operations listed in the Summary and the relevant business providing those operations.

5.2.2 Please provide a list of resilience provisions supporting the operations listed above (e.g. recovery time objectives, recovery point objectives), as related to the business providing those services.

5.2.3 Please describe your Business Continuity Plan (BCP) and frequency of testing, as relevant to the provision of the critical operations listed in the Summary and the business providing those services.

5.2.4 Please describe your Disaster Recovery (DR) testing approach and frequency of testing, as relevant to the provision of the critical operations listed in the Summary and the business providing those services.

5.2.5 Please provide a high-level overview of the ownership, review and approval process for both the BCP and DR plans, as relevant to the provision of the critical operations listed in the Summary and the business providing those services.

5.2.6 Please confirm if the BCP/DR plan and tests are reviewed externally as part of audit processes.

5.2.7 How do you incorporate material service providers into the overall BCP plan and testing?

5.2.8 Please provide a high-level overview of any actual BCP events in the last 5 years.

5.2.9 When was the last DR/BCP test completed, please provide an overview of the actions and outcomes, as relevant to the provision of the critical operations listed in the Summary.

5.3 Regulatory Compliance

5.3.1 Please describe the processes in place to ensure compliance to applicable regulations, laws, industry codes and rules (including required licences and licence regulations), as relevant to the provision of the critical operations listed in the Summary and the business providing those services.

5.3.2 Are there any key systems in place, relevant to the organisation providing the critical operations, to support the company compliance processes or issue tracking?

5.3.3 Please describe the compliance training in place for new staff and ongoing compliance training. Is there a training register maintained and who ensures it is regularly updated?

5.3.4 Have there been any regulatory review or breaches noted for the company relevant to the provision of the critical operations noted in 1.1, either potentially or in actuality?

5.3.5 Please provide a copy of your Australian Financial Services License (AFSL) and confirm equivalent licenses in your governing jurisdiction, for the relevant organisation.

5.3.6 Do you maintain an incident and complaints handling process formally? Does this include an incident and complaints register?

5.3.7 Does the Compliance team sign off or maintain a centralised library of policies and procedures for operations, trading, trade support and control functions?

5.4 Organisation Policies & Procedures

5.4.1 Please confirm if the following applicable polices are in place and if they are organisational (global or local), division or relevant business unit:

FSC Guidance Note No. 52

Policy	In Place?	Organisational, Division, or Relevant Business Unit	Date Last Reviewed
BCP Policy			
Code of Ethics			
Fraud and Corruption			
Privacy Policy			
Third Party or Vendor Management Policy or Framework			
Risk Management Policy			
Anti-Money Laundering/Counter Terrorism Financing			
Outsourcing			
Complaints Management			

5.4.2 Please outline the process for the maintenance of the review cycle, owner and sign off (individual / committee) for the relevant policies listed above.

5.4.3 Is there standard training or staff awareness processes to confirm ongoing compliance to existing policies?

5.5 Audit

5.5.1 Is there an internal audit function? Is it insourced or outsourced?

5.5.2 Who are the current external auditors and how long have they been in place?

5.5.3 Please provide an overview of the audit issue management processes in place to address audit findings.

5.5.4 Please provide a high-level overview of what reporting is provided by the Internal and external audit teams to Management / Boards / Committees?

6. Service Provider Oversight

6.1 Third Party Management

6.1.1 Please document your third-party management processes, segmentation and the criteria for identifying material vendors and how they are managed or provide a copy of your material service provider policy and/or similar relevant policy

6.1.2 Please complete the following table relevant to the critical operations listed in the Summary of this document and business providing those services:

FSC Guidance Note No. 52

Material Service Provider Name	Service Provided	Does this agreement have a service level agreement?

6.1.3 What is the assessment and selection processes in place for choosing key partners or vendors/outsourced service providers?

6.1.4 What are the due diligence processes undertaken for your key providers?

6.1.5 Who is responsible for the appointment and monitoring of the Service Providers and how does the relevant business approach relationship management?

6.1.6 Do the Risk, Compliance and/or Internal Audit departments perform any assurance reviews or testing on third party risk management activities relating to material service providers?

6.1.7 How does the organisation manage concentration risk associated with the provision of third-party vendors.

6.1.8 Please provide information about how your organisation obtains controls assurance over key operational controls that are managed by its material third parties.

7. Organisational Structure

7.1 Corporate

7.1.1 Please provide a high-level overview of the company.

7.1.2 How long has the company been in operation and have there been any changes to the corporate structure in the past 5 years?

7.1.3 Please provide copies of the past 3 audited annual reports and financial accounts.

7.2 Organisation

7.2.1 Please provide a high-level organisational structure diagram showing the functional overlay and highlight any key personnel relevant to the critical operations provided as well as the teams associated with risk management and compliance.

7.2.2 Please provide an overview of the management of key person risks, as relevant to the critical operations provided, namely how the organisation ensures continuity of service when key personnel are unavailable.

7.2.3 Has the firm undergone or implemented any significant changes, relevant to the provision of its critical operations in the last two years for example, geographic relocation, replacement of systems etc. If yes, please provide a high-level overview, including any impacts to the critical operations provided.

7.3 Insurance

7.3.1 Please confirm if the organisation has the following forms of insurance and if the superannuation fund can view the certificate of currency:

- Professional indemnity
- Electronic and computer crime
- Fraud
- Cyber

7.3.2 Has your organisation been refused any of the above stated insurances over the past 5 years?

7.3.3 Please describe your background and reference checking procedures, including criminal and credit checks for new hires for both temporary and permanent positions. Please confirm if an attestation of completed background checks is available if requested.

8. Governance and Financial Position

8.1 Governance

8.1.1 Please provide a diagrammatical representation of the corporate governance structure illustrating relevant Board and Sub-Committees, including those managing issues of risk and compliance, as well any internal audit function.

8.2 Financial Position

8.2.1 Please provide the credit/senior debt rating of the relevant organisation providing the critical operations outlined in the Summary, including from which agencies these were obtained.

8.2.2 What is the relevant organisations approach to meeting any regulatory capital requirements?

8.2.3 Has the relevant organisation failed to meet its regulatory capital requirements in the last five months?

8.2.4 What is the relevant organisation's overall approach to liquidity management, including maintaining appropriate capital to fund operational risks?

8.2.5 Please explain how the loss of one or several of the relevant organisation's largest clients would impact the firm's financial stability.

9. IT Systems and Security

9.1 IT Architecture & Applications

9.1.1 Please provide details on the team structure and relevant reporting lines for the technology team including outsourced functions and how far the outsourcing reaches (for example, fourth, fifth party etc).

9.1.2 Please provide any key and relevant IT strategies and initiatives of your organisation.

9.1.3 Please describe your system and business testing processes for changes to key systems, or provide a copy of the relevant policy.

9.1.4 Do you maintain separate environments for testing?

9.1.5 Please complete the following table, relevant to the provision of the critical operations listed in the Summary and the business that is providing those critical operations.

FSC Guidance Note No. 52

Function	Key Application	Data Centre	OS	Database
Portfolio management				
Order management				
Pre-trade compliance				
Trade matching/ confirmation				
Reconciliations				
Portfolio accounting				
Investment risk management				
Governance, Risk & Compliance				

9.2 IT Support & Cyber Security

9.2.1 Please describe the relevant organisation's access management policies for applications/systems and mobile devices.

9.2.2 Please provide an overview of the system and application support model (i.e. help desk).

9.2.3 What processes are in place to monitor system activity, downtime and performance?

9.2.4 What is the backup process for key systems, applications and data?

9.2.5 Please provide a high-level overview of your cyber-attack response framework. In your response indicate which controls are applicable to which data types. Please provide an attestation that cyber-security testing is conducted on a regular basis with satisfactory results.

9.2.6 Please document your cybersecurity monitoring and incident management processes.

9.2.7 Is there standard training or staff awareness processes regarding cyber security (i.e. phishing scams).

9.2.8 Do employees have access to work emails (and other company information) through the use of personal and company issued mobile devices/tablets? If so, please provide an overview of the security oversight on these devices, including password protection requirements, and remote wipe capabilities.