asfa
the voice of super

EY
Shape the future
with confidence

ASFA-EY CPS 230

CPS 230 ‘Operational Risk Management’ - Material Service Provider Management

Guidance Note

April 2025

ASFA has been operating since 1962 as the peak policy, research and advocacy body for Australia's superannuation industry. ASFA represents the APRA regulated superannuation industry with over 100 organisations as members from corporate, industry, retail and public sector funds, and service providers.

We develop policy positions, Guidance Notes and practice guidance through collaboration with our diverse membership base and use our deep technical expertise and research capabilities to assist in advancing outcomes for Australians.

The Association of Superannuation Funds of Australia Limited (ASFA)
PO Box 1485, Sydney NSW 2001
T +61 2 9264 9300 or 1800 812 798 (outside Sydney)

ABN 29 002 786 290
ACN 002 786 290

www.superannuation.asn.au

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multidisciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

Contents

1 About this Guidance Note

This Guidance Note is the result of a collaboration between The Association of Superannuation Funds of Australia Limited (ASFA) and EY.

The Guidance Note is general in nature and does not consider all nuances that may exist. It is intended as a guide only and is not intended to be used as a substitute for professional advice. ASFA and EY expressly disclaim all liability and responsibility to any person who relies, or partially relies, upon anything done, or omitted to be done, by this publication.

The Guidance Note does not repeat or duplicate all relevant legislation. There may be additional standards set by regulatory instruments relevant to the management of material service provider arrangements. Where they overlap or are inconsistent with this Guidance Note, the legislation or regulatory instrument will prevail.

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

It is the responsibility of each individual APRA-regulated entity to conduct their own independent assessment and, if necessary, obtain their own independent advice on the regulations to ensure compliance. APRA's regulated entities approach to operational risk must be suitable for their size, business mix, and complexity.

This paper 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.

2 Background

In July 2023, the Australian Prudential Regulation Authority (APRA) released the final Prudential Standard CPS 230 ‘Operational Risk Management’, and subsequently the accompanying Prudential Practice Guide (PPG) CPG 230 in June 2024.

CPS 230 aims to enhance the management of operational risks, improve responses to business disruptions, and manage risks associated with service providers for APRA-regulated entities. The objective is to enhance the resilience of the financial sector by ensuring that entities have robust frameworks in place to identify, assess, and mitigate operational risks.

In today’s financial services landscape, service providers (‘service providers’) play an increasingly important role in delivering core business processes. Financial services companies rely on these external partners to enhance efficiency, drive innovation, and provide specialised expertise, thereby delivering significant value to their clients. However, this dependence on service providers also introduces substantial operational risks, as evidenced by several high-profile public disruptions in recent years.

Recognising the critical need to manage these risks, CPS 230 explicitly mandates that APRA-regulated entities must understand and manage the risks associated with their service provider arrangements

3

The purpose of the guidance

The purpose of this guidance is to assist superannuation entities ('Entities') to address the CPS 230 requirements related to Material Service Providers ('MSPs').

CPS 230 identifies Material Service Providers as "those on which the entity relies to undertake a critical operation or that expose it to material operational risk"; and Material Arrangements as "those on which the entity relies to undertake a critical operation or that expose it to material operational risk".

Although there is no single globally accepted approach for managing service provider risks, there are several recognised risk management frameworks that typically focus on specific risk domains. For example, the NIST Cybersecurity Framework and ISO standards 27001, 27002, and 27018 include guidelines for managing third-party risks

This Guidance Note reflects an approach based on EY's Third Party Risk Management which has, in its formulation, considered these other frameworks.

While the Guidance Note focuses on compliance with MSP requirements, Entities may also apply it to their management of non-material service providers.

The Guidance Note may also be used by a service provider to an RSE to understand their expectations when providing services.

4 EY Third-Party Risk Management Framework

The risk associated with the use of MSPs should be an integral part of an entity’s overall risk management framework. This includes the requirement to maintain a comprehensive service provider policy that must cover how the entity will identify service providers and manage service provider arrangements, including the management of material risks associated with these parties.

EY’s Third Party Risk Management (TPRM) framework (see Figure 1) has been designed to provide effective oversight and management of service provider relationships, ensuring that risks are effectively identified, assessed, and mitigated.

The framework is structured around three key domains:

- Oversight & Governance supported by policies and procedures: This includes the framework, and roles and responsibilities establishment to ensure the effective oversight, management, and control of service provider relationships. It is supported by a service provider policy and procedures to operationalise the governance principles.

- The Lifecycle: This encompasses the end-to-end process of managing service provider relationships, from planning and due diligence through to ongoing monitoring and termination.

- Supporting Tools: These encompass the tools and technology such as the service provider inventory/register, risk profiling, reporting, and processes that collectively support the effective implementation and management of the TPRM framework and Lifecycle processes.

4

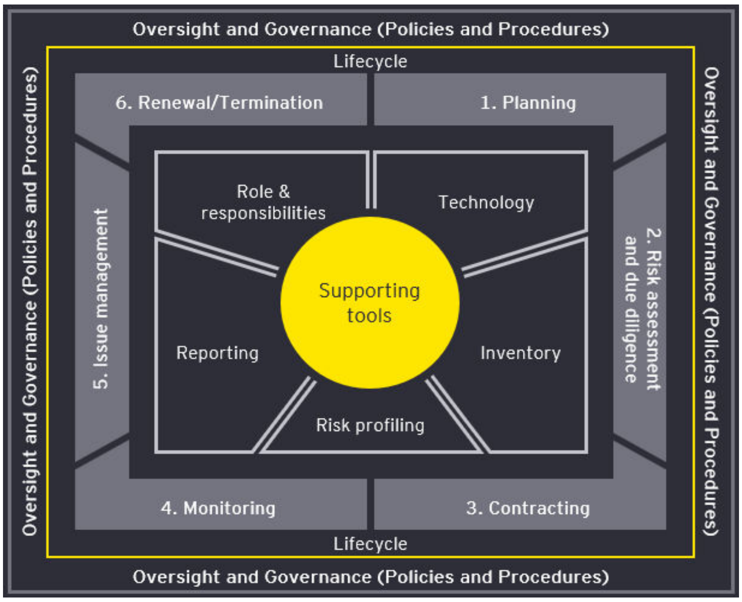
Oversight and Governance (Policies and Procedures)
Lifecycle
6. Renewal/Termination
1. Planning
Role & responsibilities
Technology
Supporting tools
Reporting
Inventory
Risk profiling
5. Issue management
2. Risk assessment and due diligence
4. Monitoring
3. Contracting
Lifecycle
Oversight and Governance (Policies and Procedures)
Oversight and Governance (Policies and Procedures)
Oversight and Governance (Policies and Procedures)

FIGURE 1: EY THIRD PARTY RISK MANAGEMENT FRAMEWORK

In this section, we consider each domain of the EY Third Party Risk Management Framework and relevant activities to be undertaken, which take into account CPS 230 requirements.

4.1 Oversight & Governance supported by Policies and Procedures

<table>
<tr><td><b>Objective</b></td><td>To establish a comprehensive TPRM Governance Framework that ensures the effective oversight, management, and control of service provider relationships across the three lines of defence. This framework aims to protect the entity from potential risks, ensure compliance with regulatory requirements, and align service provider activities with the entity’s strategic goals and operational standards.</td></tr>
<tr><td><b>Relevant CPS 230 paragraphs</b></td><td>Para 20, 21, 22, 47, 48, 49, 51, 58, 59, 60</td></tr>
<tr><td colspan="2"><b>Key activities:</b>
• Prepare/update a Board approved policy to outline the principles, objectives and guidelines for appointing service providers and managing service provider relationships. Include how the entity will identify MSPs and manage the service provider arrangements, including any material risks associated with contracting with the service provider.
• Prepare/update procedures to cover each step in the service provider lifecycle including referencing Supporting Tools. (Refer to section ‘TPRM service provider lifecycle management’ for each lifecycle phase).
• Define scope, roles, and responsibilities of various stakeholders involved in the service provider management. Refer to Appendix B for an example of a high-level roles and responsibilities across the lifecycle management, covering planning, risk assessment, contracting, monitoring, issue management, and renewal/termination.
• Develop/update training and (ongoing) awareness programs to educate employees on service provider management practices, policies and their roles and responsibilities.
• Establish communication channels and reporting mechanisms to monitor the arrangements. Incorporate APRA notification (such as notifications relating to entering into service provider agreements) and APRA reporting requirements (for example – submitting a register of material service providers on an annual basis).
• Incorporate Internal Audit obligations into the Internal Audit Plan to review any proposed material arrangement and its compliance with the service provider management policy</td></tr>
<tr><td><b>Key output/ deliverables</b></td><td>• TPRM Governance Framework providing effective oversight management, and control of third-party relationships.
• Comprehensive set of policies, procedures and practices to operationalise the service provider relationship across its lifecycle supplemented by Supporting Tools.</td></tr>
</table>

4.2 TPRM service provider lifecycle management

4.2.1 Planning

Objective	To establish a clear foundation and strategic approach for engaging with service providers. It sets the stage for all subsequent phases—risk assessment/due diligence, contracting, monitoring, issue management, and renewal/termination—by ensuring that the entity's needs, expectations, and risk management strategies are clearly defined and effectively aligned with its overall objectives. This stage aims to ensure the engagement of service providers is based on a clearly defined business need and that potential risks are identified and managed from the outset.
Relevant CPS 230 paragraphs	Para 47, 48
Key activities: • Identify Business Need and define specific requirements for the service required from a service provider, define the scope of the service provider engagement and establish the objectives of the service provider relationship reflecting key stakeholder requirements. • Establish a selection process and criteria for selecting service providers, including factors such as financial stability, reputation, expertise, and compliance with regulatory requirements. • Obtain necessary approvals from relevant stakeholders to proceed with the third-party engagement.	
Key output/ deliverables	• Decision made on whether to proceed to a due diligence phase with a service provider based on updated Business Case and results of the selection process.

4.2.2 Risk assessment and due diligence

Objective	To systematically identify, evaluate, and mitigate potential risks associated with engaging service providers. This step ensures that the entity understands the risk landscape, assesses the impact and likelihood of various risks, and implements appropriate controls to manage these risks effectively. The goal is to protect the entity from potential disruptions, financial losses, regulatory penalties, and reputational damage that could arise from third-party relationships.
Relevant CPS 230 paragraphs	Para 49, 53, 56, 59

Key activities

- Conduct an inherent risk assessment to identify, evaluate, and understand the potential risks associated with outsourcing services to the MSP before any controls or mitigations are applied. Consider the following risk domains when assessing the inherent risk of using an MSP:
  - Financial Risk: The potential for loss due to a service provider's financial instability, including insolvency, bankruptcy, or fluctuations in market conditions that could impact their ability to fulfill contractual obligations.
  - Environmental, social, and governance (ESG) Risk: Risks associated with a service provider's practices regarding environmental sustainability, social responsibility, and corporate governance, which can affect their reputation and operational viability.
  - Info Security / Cyber Risk: The risk of unauthorised access, data breaches, or cyberattacks that could compromise sensitive information or disrupt services provided by the service provider.
  - People Risk: The risk arising from the service provider's workforce, including issues related to employee turnover, skills shortages, or unethical behaviour that could impact service delivery and compliance.
  - Transaction Processing Risk: The risk of errors or failures in the service provider's transaction processing systems, which could lead to financial losses, operational disruptions, or regulatory penalties.
  - Business Continuity Risk: The risk that a service provider may not be able to continue operations in the event of a disaster or significant disruption, potentially affecting service delivery and business operations.
  - Reputational Risk: The potential for negative publicity or loss of member trust due to the service provider's actions, practices, or failures, which can impact the financial institution's reputation.

4.2.2 Risk assessment and due diligence contd.

- AML CTF Risk: The risk associated with a service provider's potential involvement in money laundering (AML) or counter-terrorism financing (CTF) activities, which could expose the financial institution to legal and regulatory penalties.
- Concentration Risk: The risk of over-reliance on a single service provider or a small group of service providers, which can lead to significant operational disruptions if those service providers fail or face challenges.
- Regulatory Compliance Risk: The risk that a service provider may fail to comply with applicable laws, regulations, or industry standards, potentially leading to legal penalties or reputational damage for the financial institution.
- Data Privacy Risk: The risk of unauthorised access to or misuse of personal data handled by the service provider, which can lead to legal liabilities and loss of customer trust.
- Geographic Location Risk: The risk associated with the service provider's location, including political instability, natural disasters, or economic conditions that could impact their ability to provide services reliably.

Below is an example of inherent risk ratings for example MSPs covering relevant risk domains:

Risk Domains	Fund Administration	Investment management	Internal audit
Financial Risk	High	High/Low*	Low
Environmental, social, and governance (ESG) Risk	Low	High	Low
Info Security / Cyber Risk	High	Low	High/Low*
People Risk	High	Low	Low
Transaction Processing Risk	High	Low	Low
Business Continuity Risk	High	High/Low*	Low
Reputational Risk	High	High/Low*	Low
AML CTF Risk	High	High/Low*	Low
Concentration Risk	High	Low	Low
Regulatory Compliance Risk	High	Low	Low
Data Privacy Risk	High	Low	Dependent on data retained by IA
Geographic Location Risk	Low	Low	Low

* Risk rating depending on materiality of the investment and investment management agreement.

4.2.2 Risk assessment and due diligence contd.

The risk rating will typically be based on entity's operational risk framework and the result of evaluating the likelihood of the risk occurring and the impact on the entity.

- Perform a due diligence assessment of the MSP's controls, processes, and capabilities to mitigate identified risks for all services they provide to the entities, based on the inherent risk assessment results.
- It is expected that rather than looking at a service provider's overall operational risk management framework, entities may limit the assessment to target the above risk domains.
- Not all the risk domains may be relevant to each service provider; therefore, the due diligence process should focus on the risk domains relevant to each service provider's services. As the nature of services varies significantly between service providers, the due diligence process should concentrate on relevant and in-scope risks. For instance, an Internal Auditor MSP relationship will be evaluated differently than an administrator based on the inherent risks identified, which will ultimately influence the level of assurance the entity needs to obtain from the service provider.
- Obtain relevant evidence from the MSP to evidence the operation of the controls, processes and capabilities. The nature and extent of the assessment is to identify any capability gap that may prevent the MSP from meeting the entities' tolerance levels and identify material operational risks. This activity should consider each relevant risk domain based on the results of the inherent risk assessment and may include the following in relation to business continuity risk:
    - Business process information relevant to the service provided to entities
    - Recovery Time and Point Objectives (RTO and ROP) and tolerance levels (if defined) for the relevant services to the entities
    - Business continuity plan (either key artefacts or entire plan) and associated testing results
    - Disaster recovery plan and its testing results
    - Control assurance reports.
    - Service Level Agreements (SLAs) and vendors' performance monitoring reports

4.2.2 Risk assessment and due diligence contd.

In assessing business continuity risk, the substitutability of the service provider should also be cconsidered – for example, whether the service can be easily substituted either by performing the service in-house or transferring to another service provider without a disruption causing material adverse impact to members. This is to understand the extent of reliance on the service provider to support minimum service levels, meet impact tolerance levels and level of assurance to be obtained from the service provider.

In relation to the control assurance reports mentioned above, these provide valuable insights into how service providers mitigate risks through their internal controls, particularly in cases where access to source evidence is restricted. When available, these reports can offer details regarding the design and effectiveness of controls related to business controls supporting critical operations, operational risk management controls, and business resilience.

By reviewing these reports, entities can assess the robustness of the service provider's control environment and determine whether the controls are adequate to manage the identified risks arising from the inherent risk assessment. For service providers that support multiple APRA-regulated entities, issuing sufficient control assurance reports can help reduce compliance costs and enhance confidence in the use of their services. Please refer to Appendix A for types of reports and considerations in evaluating control assurance reports.

- In the event that service providers do not provide the required information (for example, a controls assurance report or evidence supporting their BCP capabilities), entities should consider alternative approaches to perform their due diligence assessment, as follows:
  - Entities may perform their own due diligence by assessing the service provider's business continuity capabilities through alternative means, such as interviews, site visits, or independent assessments
  - Entities should conduct a risk assessment to evaluate the potential impact of not having the required information. This may involve analysing the criticality of the service provider's services and the associated risks, and obtaining approval form the appropriate senior governance forums on the approach
  - If the service provider is unresponsive or unable to provide the necessary information, Entities may escalate the issue to higher management within the service provider's entity
  - If a service provider consistently fails to meet information requests or demonstrate adequate business continuity capabilities, Entities may consider seeking alternative providers who can meet their compliance and risk management needs.
  - Entities should have contingency plans in place to address potential disruptions caused by inadequate service provider capabilities, ensuring they can maintain operations and comply with regulatory requirements.

4.2.2 Risk assessment and due diligence contd.

- Based on the completed due diligence assessment, determine the residual risks and review results in line with the entity's risk appetite and tolerance, and document and communicate risk findings to relevant stakeholders. Where appropriate, formulate strategies and action plans to mitigate identified risks, including implementing new or additional controls, contingency plans and monitoring mechanisms.
- Obtain necessary approvals from senior management and other relevant authorities for the proposed risk mitigation strategies and action plans.
- Use the risk assessment findings to make informed decisions about proceeding with the third-party engagement, negotiating contract terms, and implementing controls.
- Notify APRA:
  - "as soon as possible and not more than 20 business days after entering into or materially changing an agreement for the provision of a service on which the entity relies to undertake a critical operation; and
  - prior to entering into any material offshoring arrangement, or when there is a significant change proposed to the arrangement, including in circumstances where data or personnel relevant to the service being provided will be located offshore."
- We note that entities adopting CPS 230 for the first time must evaluate their current vendor relationships to identify which service providers qualify as MSPs. This assessment will involve determining whether the inherent risks linked to the services offered pose a significant operational risk or impact critical operations using the same criteria when a new service provider is evaluated. Consequently, some service provider services that are currently deemed to have low inherent risk may need to be reclassified as high risk for example due to the reliance on the service provider for critical operations and be treated as MSP going forward.

Key output/ deliverables	• MSP inventory and vendor register maintained and updated with latest vendor information relevant to MSP following APRA's required template • Residual risk profile of the (prospective) service provider based on the inherent risk assessment and informed by the due diligence information collected. • Decision whether to engage the service provider. • Ongoing monitoring procedures to be applied to MSPs

4.2.3 Contracting

Objective	To formalise the relationship between the entity and the service provider through a legally binding agreement for all material arrangements. This step ensures that all terms and conditions, including those related to risk management, compliance, performance expectations, and responsibilities, are clearly defined and agreed upon by both parties. The contracting step is crucial for protecting the entity's interests, mitigating potential risks, and ensuring that the service provider delivers the required services in a manner that aligns with the entity's standards and regulatory requirements.
Relevant CPS 230 paragraphs	Para 53, 54, 55, 56

Key activities:

- Obtain a legally binding agreement. This includes specifying the services covered, associated service levels, and setting out the rights, responsibilities, and expectations of each party. It must also include provisions to ensure the entity can meet its legal and compliance obligations, require notification of any sub-contracting arrangements, assigning liability for any failures to the service provider and include "force majeure" and termination provisions. The agreement must allow APRA access to relevant documentation and the right to conduct on-site visits, ensuring the service provider does not impede APRA's regulatory duties.

- Incorporate provisions to support ongoing monitoring, notification and review requirements under CPS 230 such as:

  Performance Monitoring:

  - Service Level Agreements (SLAs) with Key Performance Indicators (KPIs): Clearly defined performance metrics and standards that the service provider is required to meet.

  - Performance Reporting: Requirements for regular performance reports from the service provider, detailing their adherence to the SLAs and any deviations.

  - Review Meetings: Scheduled review meetings between the entity and the service provider to discuss performance, address issues, and plan improvements.

  Risk Management and Compliance:

  - Risk Assessment Updates: Provisions for periodic risk assessments to identify and evaluate any new or emerging risks associated with the service provider engagement. Additionally, requirements for the service provider to regularly provide reports on their control environment, detailing the effectiveness of their internal controls and any changes or improvements made.

  - Compliance Reporting: Requirements for the service provider to regularly report on their compliance with relevant laws, regulations, and industry standards.

  - Audit Rights: The right for the entity to conduct audits or inspections of the service provider's operations, processes, and controls to verify compliance and performance.

4.2.3 Contracting

Incident Management and Notification:

- Incident Reporting: Specifying the types of incidents that require notification, reporting timelines, and the minimum information to be reported. Clear procedures for the service provider to promptly report any incidents, breaches, or disruptions that could impact the entity.
- Notification Timelines: Specific timelines for incident notification, ensuring that the entity is informed as soon as possible.
- Incident Response: Requirements for the service provider to cooperate with the entity in investigating and resolving incidents, including providing necessary information and support.

Fourth Parties

- Fourth party notification: requirements to notify the entity by the service provider of its use of other material service providers that it materially relies upon in providing the service to the APRA-regulated entity through sub-contracting or other arrangements.
- Fourth party accountability: Stipulations that the service provider is responsible for the performance and compliance of any forth parties used in the provision of the services.

Business Continuity and Disaster Recovery:

- Business Continuity Plans (BCPs): Requirements for the service provider to maintain and regularly test their business continuity and disaster recovery plans.
- BCP Reporting: Regular updates from the service provider on the status and effectiveness of their BCPs, including test results and any changes made, ensuring that the service provider meets the defined RTOs and RPOs, along with regularly performing a Business Impact Analysis (BIA) for the services provided by service provider to the entity.
- Coordination: Provisions for coordinating business continuity efforts between the entity and the service provider to ensure seamless recovery in the event of a disruption including provisions to support the entity's business continuity and disaster recovery efforts.

Contractual Provisions for Review and Updates:

- Review Clauses: Provisions for regular reviews of the agreement to ensure it remains relevant and effective in addressing the entity's needs and regulatory requirements.
- Amendment Procedures: Clear procedures for amending the agreement, including the process for making changes and obtaining necessary approvals.
- Termination and Exit Strategy: Conditions under which the contract can be terminated, including the right to terminate for cause or convenience, and an exit strategy to ensure a smooth transition of services and data.

4.2.3 Contracting contd.

<table>
<tr><td colspan="2">‣ Information Sharing and Collaboration: Agree on appropriate information sharing and collaborations mechanisms within contractual arrangements. This includes joint or service-provider-facilitated testing on resilience outcomes, planning for exit (including standard exit clauses), and disorderly/stressed exit planning (for example, Code of Escrow).
‣ Deviation from Standard Requirements: Establish rules for deviation from standard contractual requirements and determine contingencies or mitigants needed internally for agreeing to these changes. For example, where there is no right to directly audit, consider access to third-party audit reports.
Note that where an entity has pre-existing contractual arrangements in place with a service provider, the requirements in this Prudential Standard will apply in relation to those arrangements from the earlier of the next renewal date of the contract with the service provider or 1 July 2026.</td></tr>
<tr><td><b>Key output/ deliverables</b></td><td>• Legally binding agreement that outlines terms and conditions of the services and the performance expectations between the entity and the service provider</td></tr>
</table>

4.2.4 Monitoring

Objective	To ensure continuous oversight and evaluation of service providers to manage and mitigate risks, ensure compliance with contractual and regulatory requirements, and maintain the quality and reliability of the services provided. This step is critical for identifying and addressing issues promptly, ensuring that service provider engagements remain aligned with the entity's objectives and risk appetite, and protecting the entity from potential disruptions and adverse impacts.
Relevant CPS 230 paragraphs	Para 22, 51, 56, 58, 59, 60

Key activities

- Maintain a complete and current material service provider inventory and submit to APRA on an annual basis.
- Set up mechanisms for ongoing monitoring and review of identified risks and the effectiveness of implemented controls in line with the inherent risk assessment outcome to ensure that risk assessments are periodically updated to reflect changes in the third-party relationship, external environment, and organisational context.
- Hold review meetings with the MSPs to discuss performance against SLA/contractual provisions and any control deficiencies, address issues, and plan improvements.
- Conduct periodic audits and inspections in line with the inherent risk rating to verify the MSP's compliance with contractual obligations and SLAs, using a documented test and assessment methodology. This process should:
  - leverage the information outlined in section 4.2.2, such as available control assurance reports (refer to Appendix A for types of reports and considerations in evaluating control assurance reports);
  - review the service provider's Business Continuity Plan (BCP) and Disaster Recovery (DR) testing reports; and
  - evaluate updated BCP and DR plans to confirm that their recovery capabilities align with the entity's tolerance levels for critical operations. The assessment aims to evaluate the MSP's ability to execute the BCP, adhere to the Service Level Agreement (SLA), meet performance metrics, and fulfill notification obligations.
- Conduct joint testing with the service provider to validate the capabilities that support recovery and restoration related to the specific services they provide as part of a Critical Operation. This should be done within defined objectives and under a range of severe but plausible scenarios, such as testing the joint ability to respond to any disruption.

4.2.4 Monitoring contd.

<table>
<tr><td colspan="2">• Perform regular risk assessments of the MSP risk profile and compliance status by utilising independent audits and other forms of assurance to support ongoing monitoring and risk management efforts. Identify and evaluate any new or emerging risks associated with third-party engagement, and update risk mitigation strategies and controls as needed.
• Regular reports to senior management/Board and relevant stakeholders on the status of third-party engagements, including deviations from SLA performance metrics, root causes of performance issues and corrective actions taken, updated risk profiles and compliance status, identified new and emerging risks, control evaluation results, non-compliance issues identified, summary of audit findings, status of BCP/DR plans, including test results and alignment with established tolerance levels, and notifications of the sub-contracting arrangement and associated risk assessments.
• Internal Audit to review any proposed material arrangement involving the outsourcing of a critical operation and report on the compliance of such arrangements with the entity’s service provider management policy.</td></tr>
<tr><td><b>Key output/ deliverables</b></td><td>• Updated residual risk profile of the service provider.
• Information regarding capability and maturity of service provider supporting critical operations.
• Service provider vulnerabilities and remediation activities.
• Vendor register maintained and updated with latest vendor information</td></tr>
</table>

4.2.5 Issue management and risk treatment

Objective	Any problems, incidents, or non-compliance issues related to service providers are promptly identified, reported, and resolved. This step is critical for maintaining the integrity, reliability, and security of the services provided by third parties, as well as for protecting the entity from potential disruptions, financial losses, regulatory penalties, and reputational damage.
Relevant CPS 230 paragraphs	Para 31, 32
Key activities: • Implement processes for tracking and reporting issues related to service providers, including performance failures, compliance breaches, and security incidents In line with the broader enterprise issue management framework. • Establish clear procedures with service providers for reporting issues, including who should report, what information should be included, and how reports should be documented. • Assess the severity and impact of identified issues, prioritise them based on their potential impact on the entity, and determine the appropriate response, including any notification to regulators. • Conduct root cause analysis to understand the underlying causes of issues and identify corrective actions to prevent recurrence. • Develop and implement corrective actions to resolve issues, including immediate fixes and long-term solutions. • Implement measures to mitigate the impact of issues on the entity, including contingency plans and risk mitigation strategies and logging and actioning issues. • Communicate with relevant stakeholders about issues, their status, and resolution efforts, ensuring transparency and engagement. • Regularly review issue management processes and outcomes, identify lessons learned, and implement improvements to enhance the effectiveness of third-party risk management.	
Key output/ deliverables	• Incident management policy/procedure • Issue tracker and reports

4.2.6 Renewal/Termination

Objective	The objective of the Renewal/Termination step in the Third-Party Risk Management (TPRM) lifecycle is to systematically evaluate and decide whether to continue, modify, or terminate the relationship with a service provider. This step ensures that the decision is based on a thorough assessment of the service provider performance, risk profile, compliance status, and alignment with the entity's strategic objectives and risk appetite. Effective management of this step helps maintain the integrity and reliability of third-party engagements, mitigates potential risks, and ensures a smooth transition if termination is necessary.
Relevant CPS 230 paragraphs	Para 18, 48, 56, 59

Key activities:

- Re-assess the alignment of the service provider relationship with the entity's strategic objectives, future needs and findings from the monitoring procedures.

- Make an informed decision on whether to renew, modify, or terminate the contract with the service provider and ensure that the decision is based on a comprehensive evaluation and aligns with the entity's best interests.

- If renewing the contract, negotiate terms that reflect any changes in requirements, performance expectations, and risk management strategies, and ensure that the renewed contract addresses current and future needs, and mitigates identified risks. Also consider the potential systemic risks posed by the concentration of services provided by the service provider, including the implications of relying on a single provider for critical services.

- If terminating the contract, ensure a smooth and orderly transition of services and data to minimise disruption based on a transition plan to ensure smooth and orderly transfer of services and data based on clear exit strategies for both planned and unplanned terminations. This should include processes for transferring logical and physical assets in a timely manner and in an appropriate format, as well as ensuring that all stakeholders are aware of their roles during the transition.

- Maintain comprehensive records of the renewal/termination decision-making process, including evaluations, approvals, and contractual changes. Also implement feedback mechanisms to gather insights from the renewal or termination process. This can help identify areas for improvement in future engagements with service providers.

4.2.6 Renewal/Termination contd

<table>
<tr><td colspan="2">• Notify APRA:
‣ “as soon as possible and not more than 20 business days after entering into or materially changing an agreement for the provision of a service on which the entity relies to undertake a critical operation; and
‣ prior to entering into any material offshoring arrangement, or when there is a significant change proposed to the arrangement, including in circumstances where data or personnel relevant to the service being provided will be located offshore.”</td></tr>
<tr><td><b>Key output/ deliverables</b></td><td>• Developed and validated renewal/exit strategies
• Risk and performance-based decision to renew/modify or terminate service provider arrangement in accordance with the entity’s strategic objectives.</td></tr>
</table>

4.3 Supporting tools

A number of supporting tools can be used to support the TPRM service provider lifecycle management, which include:

- Service provider Inventory/register

Description: The inventory maintains a comprehensive and up-to-date list of all third parties engaged by the entity. This inventory includes critical details such as the nature of the relationship, the services provided, risk ratings, contract status, and other relevant information (for example, active, offboarded, inactive, third-party lifecycle phase, detailed due diligence status, any fourth parties). Supplier subcontractors (fourth parties) are also identified, documented and tracked within the inventory capturing key standardised metadata (for example, geographic location – country, city) to provide transparency into fourth parties and associated concentration and subcontractor risk across supplier population.

The inventory serves as a central repository for tracking and managing third-party relationships. APRA has published a material service provider register template. Entities should ensure their register of third parties is updated to align with the information requested in the template to support ongoing APRA reporting requirements.

- MSP assessment methodology

Description: The methodology is a critical tool designed to assess the materiality of service providers in accordance with CPS 230 requirements. It outlines a series of targeted questions and criteria that evaluate various aspects of the service provider's materiality. Key considerations include assessing whether the service provider delivers prescribed services and whether it is relied upon for Critical Operations. By systematically gathering this information, entities can ensure that their service providers meet the necessary thresholds for materiality and can support informed decision-making regarding the selection and ongoing evaluation of service providers.

4.3 Supporting tools contd.

- Risk Profiling

Description: Risk profiling involves assessing and categorising the risk associated with each service provider based on various factors such as the nature of the services provided, the service provider's financial stability, regulatory compliance, and potential impact on the entity. This process helps in identifying high-risk third parties and prioritising risk management efforts accordingly. An Inherent Risk Questionnaire (IRQ) plays a crucial role in this assessment by gathering information about potential risks related to a service provider's operations, processes, and external dependencies. The IRQ typically includes questions about the provider's business practices, compliance with regulations, financial stability, and any past incidents of risk or failure. By systematically assessing these factors through the IRQ, entities can gauge the level of inherent risk posed by each service provider, thereby enhancing their risk profiling efforts.

The IRQ is specifically designed to identify inherent risks (operational, compliance, reputational), facilitate informed decision-making regarding service provider engagement, and ensure compliance with regulatory requirements, particularly CPS 230. It can be implemented via Excel or digital platforms and must be regularly updated to align with evolving standards. The inherent risk rating derived from the IRQ influences the level of oversight required, with higher ratings necessitating more stringent monitoring, while lower ratings allow for reduced efforts. Additionally, the IRQ considers residual risk, evaluating the level of risk remaining after controls are implemented, which helps entities understand their overall risk landscape and prepare for potential disruptions, ensuring a comprehensive risk management framework in line with CPS 230.

- Reporting

Description: The reporting process involves generating and disseminating reports on third-party risk management activities to relevant stakeholders. These reports may include information on third-party performance, compliance status, risk assessments, and any incidents or issues encountered. Key concentration metrics include spend, service dependency, geographic location, fourth party, usage - number of functions supported, with associated thresholds to inform management of next best steps and risk management discussions (for example, are there established contingencies for reliance on a single third-party for multiple services). Effective reporting ensures transparency and enables informed decision-making by senior management and other stakeholders.

- Technology

Description: Technology plays a vital role in supporting the TPRM framework by providing tools and systems for managing third-party relationships. This includes software solutions (for example, GRC solutions) for maintaining the third-party inventory, conducting risk assessments, monitoring third-party performance, and generating reports. Technology enables automation, enhances data accuracy, and provides real-time insights, making the TPRM process more efficient and effective.

5

Appendix A: Evaluation of service provider supplied reports on their control environment

The following table provides an overview of typical control reports and their applicability to satisfy CPS 230 requirements.

Type of control assurance reports	Background	Key Features	Level of comfort over the service provider's control environment	Operational Risk domains covered
ASAE 3150 Assurance Engagements on Controls	A controls assurance report prepared against a set of predefined objectives. The scoping of a ASAE 3150 is flexible based on the requirements of the service provider and user entities. A type 1 report covers only the design effectiveness of controls, while a type 2 report covers both design and operating effectiveness of controls.	The scope of the report is flexible based on the service provider and the user entities requirements against a set of predefined objectives.	A type 2 of this report can be tailored to the new requirements, with a mapping to MSP's internal controls to meet relevant obligations. Some service providers already provide an ASAE 3150 assurance report covering regulatory requirements under APRA's prudential standard CPS 234 on Information Security and could be extended to cover additional CPS 230 considerations.	• Transaction Processing Risk • Business Continuity Risk • Info Security / Cyber Risk • Data Privacy Risk

Type of control assurance reports	Background	Key Features	Level of comfort over the service provider's control environment	Operational Risk domains covered
GS 007 (ASAE 3402)	Guidance Statement GS 007 'Audit Implications of the Use of Service Entities for Investment Management Services' report issued under the Standard on Assurance Engagements ASAE 3402 ' Assurance Reports on Controls at a Service Organisation', provides assurance to the user entities (clients of the service organisation) and their external auditors in the context of the user entity's financial reporting that the controls at the service organisation are suitably designed and are operating effectively to meet the control objectives.	The scope of the report typically covers the business services such as registry, custody, asset management and investment administration as well as technology processes such access and change management, incident management and data back and recovery.	The scope of this report is limited to addressing controls relevant to the user entities' financial statement reporting.	• Financial Risk • Transaction Processing Risk relevant to financial reporting

Type of control assurance reports	Background	Key Features	Level of comfort over the service provider's control environment	Operational Risk domains covered
Systems and Organisation Controls (SOC) 2 & ISAE3000	A SOC 2 (System and Organisation Controls 2) report (issued under ISAE 3000) is designed to provide assurance about the controls at a service organisation that are relevant to security, availability, processing integrity, confidentiality, and privacy. SOC 2 reports are based on the Trust Services Criteria (TSC) and can cover one or more of the following principles: • **Processing Integrity:** System processing is complete, valid, accurate, timely, and authorised. • **Security:** The system is protected against unauthorised access (both physical and logical).	SOC 2 reports may include or exclude TSCs in their scope apart from the mandatory Security Common Control Criteria.	This report addresses information security controls and can be expanded to cover relevant aspects of CPS 230.	• Business Continuity Risk • Info Security / Cyber Risk • Data Privacy Risk

Type of control assurance reports	Background	Key Features	Level of comfort over the service provider's control environment	Operational Risk domains covered
	• **Availability:** The system is available for operation and use as committed or agreed. • **Confidentiality:** Information designated as confidential is protected as committed or agreed. • **Privacy:** Personal information is collected, used, retained, disclosed, and disposed of in conformity with the commitments in the entity's privacy notice SOC 2 reports come in two types: • **Type I Report:** This report provides an opinion on the fairness of the presentation of the service organisation's system and the suitability of the design of the controls as of a specific date.			

Type of control assurance reports	Background	Key Features	Level of comfort over the service provider's control environment	Operational Risk domains covered
	- **Type II Report:** This report provides an opinion on the fairness of the presentation of the service organisation's system, the suitability of the design of the controls, and the operating effectiveness of the controls over a specified period (typically six months to one year).			

Type of control assurance reports	Background	Key Features	Level of comfort over the service provider's control environment	Operational Risk domains covered
Systems and Organisation Controls (SOC) 1 & ISAE3402	A SOC 1 (System and Organisation Controls 1) report issued under the International Standard on Assurance Engagements ISAE 3402 'Assurance Engagements other than A SOC 1 (System and Organisation Controls 1) report issued under the International Standard on Assurance Engagements ISAE 3402 'Assurance Engagements other than Audits or Reviews of Historical Financial Information Reports on Controls at a Service Organisation' is designed to provide assurance to user entities and their auditors about the controls at a service organisation that are relevant to the user entities' financial reporting.	• The scope is limited to controls relevant to the user entity's financial reporting. • The Type I report does not provide an opinion on the operating effectiveness of the controls while a Type II does.	This report has its focus of the controls relevant to the user entities' financial reporting.	• Financial Risk • Transaction Processing Risk relevant to financial reporting

Type of control assurance reports	Background	Key Features	Level of comfort over the service provider's control environment	Operational Risk domains covered
	SOC 1 reports come in two types: • **Type I Report:** This report provides an opinion on the fairness of the presentation of the service organisation's system and the suitability of the design of the controls as of a specific date • **Type II Report:** This report provides an opinion on the fairness of the presentation of the service organisation's system, the suitability of the design of the controls, and the operating effectiveness of the controls over a specified period			

Type of control assurance reports	Background	Key Features	Level of comfort over the service provider's control environment	Operational Risk domains covered
ISO 27001 certificate	An ISO 27001 certificate is a formal recognition that an organisation has implemented an Information Security Management System (ISMS) that meets the requirements of the ISO/IEC 27001 standard. The certificate indicates that the service provider has a framework in place to manage information security risks and that this framework has been independently audited and found to be compliant with the standard.	• An ISO 27001 certificate covers resilience but is security focussed in nature. • It does not provide detailed information on the controls assessed; however, the certification process is supported by documentation that may provide further details on the controls implemented and assessed. Entities seeking to understand the specific controls in place should refer to these documents for detailed information. • The certificate itself does not guarantee that all controls are effectively operating. Instead, it indicates that the organisation has a framework in place to manage information security risks	This report provides a high level view of the service providers IT security control environment and does not include an evaluation of control operating effectiveness.	• Info Security / Cyber Risk

6

Appendix B: Responsibility Matrix for Service Provider Management

This chart provides an example of the high-level roles and responsibilities across the lifecycle management, with the Board being ultimately accountable for oversight of an entity's operational risk management, including approving the service provider management policy and management of service provider arrangements.

Activity	Responsible (R)	Accountable (A)	Consulted (C)	Informed (I)
Planning	Business Owner/ Procurement Team	Business Owner	Legal, Compliance, Risk Management IT Security	Executive, management committee, Board committees/Board
Risk Assessment	Risk Management	Business Owner/ Risk Management	Business Owner, Compliance, IT Security	Executive, management committee, Board committees/Board
Contracting	Legal	Business Owner	Procurement Team, Compliance, Risk Management	Executive, management committee, Board committees/Board
Monitoring	Business Owner	Business Owner	Risk Management, IT Security, Compliance	Executive, management committee, Board committees/Board Procurement
Issue Management	Business Owner	Business Owner	Risk Management, Legal, Compliance	Executive, management committee, Board committees/Board Procurement
Renewal/ Termination	Procurement Team	Business Owner	Legal, Compliance, Risk Management	Executive, management committee, Board committees/Board

Explanation of Roles:

- Responsible (R): The person or team responsible for executing the task.
- Accountable (A): The person who is ultimately accountable for the task's completion and quality.
- Consulted (C): Stakeholders who need to be consulted before a decision or action is taken.
- Informed (I): Stakeholders who need to be kept informed about the progress and outcomes.

asfa
the voice of super