DRAFT

PRUDENTIAL PRACTICE GUIDE

Draft CPG 230 Operational Risk Management

Integrated version

17 July 2023

Disclaimer and Copyright

This prudential practice guide is not legal advice and users are encouraged to obtain professional advice about the application of any legislation or prudential standard relevant to their particular circumstances and to exercise their own skill and care in relation to any material contained in this guide.

APRA disclaims any liability for any loss or damage arising out of any use of this prudential practice guide.

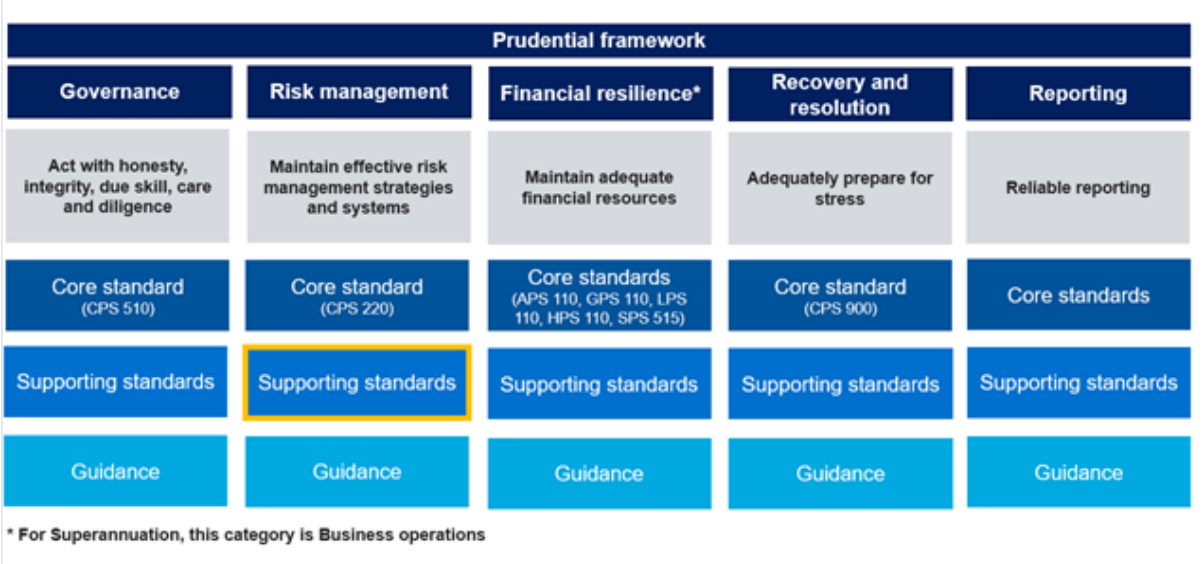
Contents

About this guide

Prudential practice guides (PPGs) provide guidance on APRA's view of sound practice in particular areas. PPGs frequently discuss legal requirements from legislation, regulations or APRA's prudential standards, but do not themselves create enforceable requirements.

This PPG sets out guidance for APRA-regulated entities to assist in complying with *Prudential Standard CPS 230 Operational Risk Management* (CPS 230). Under CPS 230, APRA-regulated entities are required to effectively manage operational risks, continue to deliver critical operations through disruptions and effectively manage the risks arising from the use of service providers.

The graphic below summarises APRA's prudential framework, and shows where CPS 230 fits in, within the Risk management pillar.



Related standards

CPS 230 replaces and supersedes five existing prudential standards: *Prudential Standard CPS 231 Outsourcing* (CPS 231), *Prudential Standard SPS 231 Outsourcing* (SPS 231), *Prudential Standard HPS 231 Outsourcing* (HPS 231), *Prudential Standard CPS 232 Business Continuity Management* (CPS 232) and *Prudential Standard SPS 232 Business Continuity Management* (SPS 232).

CPG 230 replaces and supersedes five existing PPGs: *Prudential Practice Guide GPG 230 Operational Risk* (GPG 230), *Prudential Practice Guide LPG 230 Operational Risk* (LPG 230), *Prudential Practice Guide CPG 231 Outsourcing* (CPG 231), *Prudential Practice Guide SPG 231 Outsourcing* (SPG 231) and *Prudential Practice Guide SPG 232 Business Continuity Management* (SPS 232).

APRA's prudential standards and PPGs for operational resilience are summarised below.

Operational resilience	Prudential Standard	PPGs
Operational risk management	• CPS 230	• CPG 230 • Pandemic planning (CPG 233) • Data management (CPG 235) • Fraud risk management – Superannuation (SPG 223)
Information security	• CPS 234	• CPG 234

Not all of the practices outlined in this PPG will be relevant for every entity; for example, certain guidance may be more relevant depending on the size, nature and complexity of a regulated entity's operations. Subject to meeting the requirements under CPS 230, APRA-regulated entities have flexibility in managing operational risk in a manner commensurate with the scale and complexity of their business.

This integrated version of CPG 230 maps APRA's guidance to the relevant paragraphs in CPS 230. Paragraphs from CPS 230, which are enforceable requirements, have been set out in blue boxes like this; the accompanying guidance follows below, outside the blue boxes.

Glossary

ADI	Authorised deposit-taking institution, as defined in the *Banking Act 1959*
APRA	Australian Prudential Regulation Authority
APS 001	*Prudential Standard APS 001 Definitions*
ASIC	Australian Securities and Investments Commission
BCP	Business continuity plan
Board	Board of directors
CPS 220	*Prudential Standard CPS 220 Risk Management*
CPS 230	*Prudential Standard CPS 230 Operational Risk Management*
CPS 234	*Prudential Standard CPS 234 Information Security*
GPS 001	*Prudential Standard GPS 001 Definitions*
HPS 001	*Prudential Standard HPS 001 Definitions*
LPS 001	*Prudential Standard LPS 001 Definitions*
PPG	Prudential practice guide
RSE	Registrable superannuation entity
RSE licensee	Registrable superannuation entity licensee as defined in s10(1) of the *Superannuation Industry (Supervision) Act 1993*
SIS Act	*Superannuation Industry (Supervision) Act 1993*
SPS 220	*Prudential Standard SPS 220 Risk Management*

Key principles

12. An APRA-regulated entity must:

(a) effectively manage its operational risks, and set and maintain appropriate standards for conduct and compliance;

(b) maintain its critical operations within tolerance levels through severe disruptions; and

(c) manage the risks associated with the use of service providers.

13. An APRA-regulated entity must identify, assess and manage operational risks that may result from inadequate or failed internal processes or systems, the actions or inactions of people or external drivers and events. Operational risk is inherent in all products, activities, processes and systems.

14. An APRA-regulated entity must, to the extent practicable, prevent disruption to critical operations, adapt processes and systems to continue to operate within tolerance levels in the event of a disruption and return to normal operations promptly once a disruption is over.

15. An APRA-regulated entity must not rely on a service provider unless it can ensure that in doing so it can continue to meet its prudential obligations in full and effectively manage the associated risks.

1. The aim of CPS 230 is to ensure that APRA-regulated entities ('entities') are resilient to operational risks and disruptions. Operational resilience is the outcome of prudent operational risk management: the ability to effectively manage and control operational risks and maintain critical operations through disruptions.

2. Conduct and compliance are included in CPS 230 as types of operational risk, rather than as separate material risks. Breaches of conduct and compliance are often indicative of underlying failings in internal controls in operational risk management. In maintaining appropriate standards for conduct and compliance, entities need to have robust processes and controls in place to comply with conduct regulation administered by ASIC.

3. While all requirements of CPS 230 apply to all entities, APRA expects an entity's approach to operational risk to be proportionate to its size, business mix and complexity. In particular, smaller entities may have simpler operational risk profiles with, for example, a narrower product mix and domestic focus.

4. For most smaller entities, APRA would expect a simpler approach to implementing and complying with CPS 230. This applies, in particular, to the level of granularity expected in assessing operational risk profile, including identifying and documenting processes, resources and scenario analysis. A smaller entity could identify and document its processes and resources for critical operations only at a high-level.

Risk management framework

16. As part of its risk management framework required under Prudential Standard CPS 220 Risk Management (CPS 220) and Prudential Standard SPS 220 Risk Management (SPS 220), an APRA-regulated entity must develop and maintain:

(a) governance arrangements for the oversight of operational risk;

(b) an assessment of its operational risk profile, with a defined risk appetite supported by indicators, limits and tolerance levels;

(c) internal controls that are designed and operating effectively for the management of operational risks;

(d) appropriate monitoring, analysis and reporting of operational risks and escalation processes for operational incidents and events;

(e) business continuity plan(s) (BCPs) that set out how the entity would identify, manage and respond to a disruption within tolerance levels and are regularly tested with severe but plausible scenarios; and

(f) processes for the management of service provider arrangements.

17. As part of the required reviews of the risk management framework under CPS 220 and SPS 220, an APRA-regulated entity must review its operational risk management. The reviews must cover those aspects of operational risk management set out in paragraph 16.

18. Operational risk management must be integrated into an APRA-regulated entity's overall risk management framework and processes. Business continuity planning must be consistent with, and not conflict or undermine, an APRA-regulated entity's recovery and exit planning.

19. Where APRA considers that an APRA-regulated entity's operational risk management has material weaknesses, APRA may:

(a) require an independent review of the entity's operational risk management;

(b) require the entity to develop a remediation program;

(c) require the entity to hold additional capital, as relevant;

(d) impose conditions on the entity's licence; and

(e) take other actions required in the supervision of this Prudential Standard.

5. CPS 230 builds on the general risk management requirements in *Prudential Standard CPS 220 Risk Management* (CPS 220) and *Prudential Standard SPS 220 Risk Management* (SPS 220), with specific requirements for the management of operational risks.

6. Where an entity adopts a group policy as part of its operational risk management framework, a prudent entity would ensure the policy is appropriate to its size, business mix and complexity.

7. An entity could consider maintaining a standalone operational risk management framework or incorporate operational risk into its general risk management framework. Where an entity establishes a standalone operational risk management framework, it would ensure that it is aligned with its general risk management framework. This includes, for example, ensuring that risk appetite settings, risk management strategies and governance arrangements are consistent across the frameworks.

8. A prudent entity would also ensure that, if both the business continuity plan (BCP) and recovery plan are triggered at the same time, crisis governance arrangements remain effective. This would include that communication strategies are not duplicative or inconsistent, and any triggers used for activation would not send conflicting signals.[1]

9. APRA's prudential standards for ADIs and insurers require that operational risk capital reflects the operational risk profile of the entity.[2] Generally, where there are material weaknesses in the management of operational risk, APRA expects an ADI or insurer would hold additional capital until remediation is complete. This may be through an overlay determined by senior management, required by the Board or applied by APRA.

10. Where an entity has identified material weaknesses in its operational risk management, APRA expects that the entity would keep it informed of the progress of its remediation.

11. CPS 230 requires an entity to notify APRA in the circumstances set out in Table 1. Notifications to APRA are to be made electronically using the form available on APRA's website.

---

[1] APRA's requirements for recovery and exit planning are set out in *Prudential Standard CPS 190 Recovery and Exit Planning* (CPS 190).

[2] APRA requires ADIs and insurers to hold capital for operational risks, as prescribed by *Prudential Standard APS 115 Capital Adequacy: Standardised Measurement Approach to Operational Risk* (APS 115), *Prudential Standard GPS 118 Capital Adequacy: Operational Risk Charge* (GPS 118), *Prudential Standard LPS 118 Capital Adequacy: Operational Risk Charge* (LPS 118) and *Prudential Standard HPS 118 Capital Adequacy: Operational Risk Charge*.

Table 1. Notifications to APRA

Notifications to APRA	
Operational risk incidents	As soon as possible and not later than 72 hours after becoming aware of a material incident (paragraph 33 of CPS 230)
Business continuity	As soon as possible and not later than 24 hours after a disruption to a critical operation outside of tolerance (paragraph 42 of CPS 230)
Material service providers	As soon as possible and not later than 20 business days after entering into or materially changing an agreement (paragraph 59(a) of CPS 230)
Offshoring	Prior to entering into, or when there is a significant change to, any offshoring agreement with a material service provider (paragraph 59(b) of CPS 230)

Note: A notification of an information security incident reported under *Prudential Standard CPS 234 Information Security* (CPS 234) is not required to be separately reported under CPS 230.

Roles and responsibilities

20. The Board of an APRA-regulated entity is ultimately accountable for oversight of an entity's operational risk management. This includes business continuity and the management of service provider arrangements.

21. The Board must ensure that the APRA-regulated entity sets clear roles and responsibilities for senior managers for operational risk management, including business continuity and the management of service provider arrangements.

12. As for any material risk, oversight of operational risk is ultimately the accountability of the Board. A key lesson from the *Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry* was the importance of strong oversight of non-financial risks, with the Board having the relevant information to allow it to make informed decisions. CPS 230 therefore sets out areas of specific responsibility for the Board in overseeing operational risk.

13. A prudent Board would have a clear understanding of who is accountable within the entity for which aspect of operational risk management, including business continuity and the management of service provider arrangements, and be confident that there are no gaps in accountabilities.

14. To support this, senior management would typically define roles and responsibilities with respect to operational risk management for senior management across the entity through a combination of processes, including role statements, reporting lines and charters of governing bodies. This would not be limited to the operational risk management function.

15. Best practice is for business line management to be responsible for embedding operational risk management practices, and as a result to also be the owners of the risk within the entity. In addition, there would typically be established processes for delegations, escalation of risks and issues to the Board and senior management, and defined reporting requirements.

22. The Board must:

(a) oversee operational risk management and the effectiveness of key internal controls in maintaining the entity's operational risk profile within risk appetite. The Board must be provided with regular updates on the APRA-regulated entity's operational risk profile and ensure senior management takes action as required to address any areas of concern;

(b) approve the BCP and tolerance levels for disruptions to critical operations, review the results of testing and the execution of findings; and

(c) approve the service provider management policy, and review risk and performance reporting on material arrangements.

23. Senior management of an APRA-regulated entity must provide clear and relevant information to the Board on the expected impacts on the entity's critical operations when the Board is making decisions that could affect the resilience of critical operations.

16. To provide effective oversight of the operational risk profile of an entity, APRA expects that a Board would typically:

    a) review and challenge regular updates to the operational risk profile that cover the full range of operational risks in a clear and concise way. This could be through the use of indicators, limits and tolerance levels to ensure that areas that are at risk or outside of appetite are brought to the Board's attention and remediated as appropriate;

    b) regularly review and challenge the effectiveness of the key internal control environment that impacts the operational risk profile;

    c) deep dive into any areas of significant weakness and be kept actively informed of progress in major remediation programs;

    d) pay particular attention to significant new ventures that may give rise to material or novel operational risks, such as activities associated with crypto assets; and

    e) ensure internal audit provides robust assurance on operational risk, with sufficient coverage in the audit plan, and appropriate skills and capabilities. Better practice would be for a Board to also consider where further assurance is needed, including through expert opinion or other means.

17. Where an entity has multiple, more detailed, plans that sit underneath the overall BCP, these may be approved by senior management as long as they are consistent with, and aligned to, the overall BCP. An example of this approach may be a Board-approved entity-wide BCP, which is supported by senior management-approved divisional BCPs.

18. While the Board approves the entity's overall tolerance levels, senior management are able to set more granular tolerance levels and indicators that would be consistent with, and not undermine, the Board-approved levels.

19. An example of this approach for an ADI could be a Board-approved tolerance level for payments, with more granular senior management-approved tolerance levels for specific types of payments in particular jurisdictions. For an insurer, there may be a Board-approved tolerance level for claims processing, with more granular senior management-approved tolerance levels for specific parts of the claims processes.[3] For superannuation, more granular tolerances may be set for parts of the investment and fund administration processes, such as for the timely investment of contributions and any payments that may have a direct impact on members (such as retirement benefits or early release payments for severe financial hardship and processing of rollovers).

20. While the Board of an APRA-regulated entity is required to approve the entity's service provider management policy, the Board is not expected to authorise every subsequent change to the service provider management policy, unless those changes are material in in nature.

21. APRA has observed that Boards have not consistently been provided with important information on operational risk when making strategic decisions. APRA expects that information provided to the Board be targeted, relevant and sufficient for directors to clearly understand the potential impact on the operational resilience of an entity's critical operations based on the decisions they make. This could include, for example: a material acquisition or merger; a new venture into new products or markets; the implementation of a new core technology platform; or, for insurers, the outsourcing of claims management or underwriting.

[3] Insurers may have an outage limit for an automated renewals system, as there could be a risk of writing unintended business, or business at a price or coverage level beyond their risk appetite. In such an example, senior management might approve a shorter tolerance level for system outages than the Board-approved level if the outage is considered to significantly impact their business.

Operational risk management

24. An APRA-regulated entity must manage its full range of operational risks, including but not limited to legal risk, regulatory risk, compliance risk, conduct risk, technology risk, data risk and change management risk. Senior management are responsible for operational risk management across the end-to-end process for all business operations.

25. An APRA-regulated entity must maintain appropriate and sound information and information technology (IT) capability *to meet its current and projected business requirements and to support its critical operations and risk management. In managing technology risks, an APRA-regulated entity must monitor the age and health of its information assets and meet the requirements for information security in Prudential Standard CPS 234 Information Security (CPS 234).*

22. There are a broad range of operational risks. While CPS 230 defines, at a high-level, a range of operational risks to be managed, it is the responsibility of the entity to ensure that it captures, defines and manages all specific operational risks that are most relevant to its particular business mix.

23. CPS 230 uses a principles-based approach to operational risk management that is outcomes-focussed, and reflects that:

    a) the management of operational risk is foremost the responsibility of the entity's business lines, and ideally is embedded within the respective business;

    b) senior managers within the business are responsible for the ownership and management of operational risk across an entity's end-to-end process; and

    c) the Board is ultimately accountable for the oversight of operational risk management and is expected to ensure that senior management effectively manages the risks.

24. APRA expects that senior management would ensure that the operational risk management framework operates effectively and is regularly updated. This may involve end-to-end business process mapping conducted across all business operations, including those performed by service providers.

Operational risk profile and assessment

26. An APRA-regulated entity must assess the impact of its business and strategic decisions on its operational risk profile and operational resilience, as part of its business and strategic planning processes. This must include an assessment of the impact of new products, services, geographies and technologies on its operational risk profile.

25. New products, or changes that materially alter the nature of a product offering, typically impact an entity's operational risk profile and may require changes to controls and risk

management processes. Entities also have other obligations for new products, such as meeting ASIC's design and distribution obligations.

26. The business case for strategic initiatives involving new products, services, geographies, and technologies, would typically be accompanied by a formal assessment informing senior management and the Board of the risk impacts. This assessment would outline the inherent risk, planned controls and residual impact on the operational risk profile, as well as any proposed risk appetite settings. Better practice is for such an assessment to be made for any business or strategic decision which materially impacts an entity's operational risk profile, including changes that significantly alter its operating model.

27. Emerging technologies may result in novel operational risks for entities. Better practice is for these risks to be considered on a regular basis, so that appropriate controls are put in place, together with robust management and monitoring.

28. For activities associated with crypto-assets, operational risk management is particularly important, and encompasses heightened risks in relation to fraud, cyber, conduct, financial crime and technology.[4] APRA expects that entities will conduct appropriate due diligence and a comprehensive risk assessment before engaging in activities associated with crypto-assets and apply robust risk management controls. Better practice would also be to treat any service providers that are relied upon for such activities as material, given the novel operational risks that they give rise to.

27. An APRA-regulated entity must maintain a comprehensive assessment of its operational risk profile. As part of this, an APRA-regulated entity must:

(a) maintain appropriate and effective information systems to monitor operational risk, compile and analyse operational risk data and facilitate reporting to the Board and senior management;

(b) identify and document the processes and resources needed to deliver critical operations, including people, technology, information, facilities and service providers, the interdependencies across them, and the associated risks, obligations, key data, and controls; and

(c) undertake scenario analysis to identify and assess the potential impact of severe operational risk events, test its operational resilience, and identify the need for new or amended controls and other mitigation strategies.

29. An entity would frequently reassess its operational risk profile to reflect any changes in strategy, risk profile or business mix.

[4] There may also be novel risks inherent in the crypto-asset or network, such as risks arising from the use of third parties for redemption and operation, or through the use of custodians, crypto infrastructure providers, exchanges or wallet providers. Specific consideration should be given to the risks around fraud and asset security, including the potential for the loss or theft of private keys, wallets containing funds and authentication devices. For further advice, see *Crypto-assets: Risk management expectations and policy roadmap* (APRA, 21 April 2022).

30. Data quality is an important input into the comprehensive assessment, to ensure an accurate and reliable operational risk profile is produced.

31. Better practice is for information systems to enable real time and aggregated reporting and integrate risk data across different components of the framework, for example: risks, obligations and key data (including controls, issues, incidents and breaches).

32. A prudent entity would consider what data it relies on as part of the processes to deliver critical operations. Better practice would be to consider key data that form part of the process and ensure that the data risk is managed appropriately.

33. An entity could use self-assessments to inform the overall comprehensive assessment of its operational risk profile. Typically, self-assessments include the steps outlined in Table 2.

Table 2. Operational risk: Self-assessment stages

Operational risk: Self-assessment stages	
1. Context	Considering the business environment and changes within the business
2. Risk identification	Identifying and recording operational risks within the business, including causes and inherent and residual ratings
3. Controls identification	Identifying and recording controls used to mitigate operational risks and assess the design and operating effectiveness of these controls, including testing results and any gaps and weaknesses
4. Risk appetite	Assessing performance against risk appetite
5. Actions	Developing actions or remediation plans, including risk acceptance where appropriate, to address higher rated risks and those exceeding risk appetite

34. Better practice in self-assessments includes:

a) implementation across the whole entity, encompassing all business activities, products, and services;

b) identification of linkages across all components of the framework (such as risks, obligations, key data and controls);

c) allocation of risks and controls to owners at an appropriate level of seniority to manage the risks;

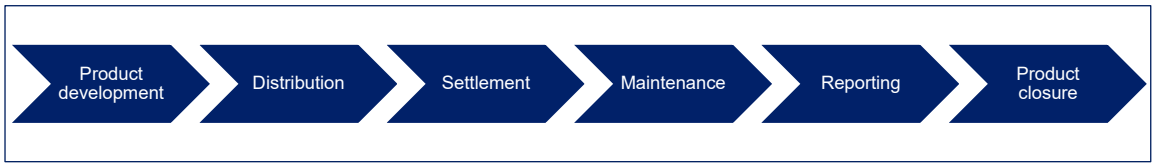
d) clear records and substantiation of assessments, including information on actual events;

e) clear escalation protocols for risks requiring Board and senior management action, including formal acceptance of risks and actions that are higher rated or exceeding appetite; and

f) aggregation to support oversight by senior management and the Board.

35. Effective operational risk management relies on a thorough understanding of an entity's business processes. Clearly defining the end-to-end processes, as set out in Figure 1 below, enables an entity to identify risks, obligations, key data and controls.

Figure 1. End-to end process view of critical operations



36. Better practice in identifying and documenting end-to-end processes and resources would include:

    a) a structured approach to map out an end-to-end view of processes for each critical operation, including people, technology, information, facilities and service providers needed for the operation;

    b) use of these maps to identify risks, obligations, key data and controls, as well as interdependencies;

    c) identifying owners and establishing clear lines of accountability for risks, obligations, key data and controls, as well as for issues or incidents that arise;

    d) reviewing maps for completeness and accuracy and keeping them updated where there are changes in the business or risks; and

    e) identifying and documenting end-to-end processes for operations that are not necessarily critical but nevertheless expose an entity to material operational risk, such as distribution channels.

37. Scenario analysis is an important part of the assessment of operational risk, enabling an entity to consider potential changes to its operating environment and inherent risk profile. APRA expects that a prudent entity would ensure that its scenarios provide sufficient coverage and adequate understanding of financial and operational resilience impacts from severe but plausible operational risk events.

38. Impacts from scenario analysis are also expected to be considered in evaluating the coverage of risks captured in an entity's risk profile, in addition to the current health of the control environment and mitigation strategies.

39. APRA expects that prudent entities would ensure the scenarios used are sufficiently stressed to test the suitability of the risk and control environment. Where issues are identified the entity would be expected to take appropriate corrective action. Better practice would be for an entity to use a documented procedure to conduct its scenario analysis and update its scenarios at least annually.

40. Larger entities would generally undertake separate scenario analysis exercises, with standalone reports. Smaller entities would typically evaluate operational risk scenarios as part of their strategic and business planning process.

28. An APRA-regulated entity must conduct a comprehensive risk assessment before providing a material service to another party to ensure that the APRA-regulated entity is able to continue to meet its prudential obligations after entering into the arrangement. APRA may require an APRA-regulated entity to review and strengthen internal controls or processes where APRA considers there to be heightened prudential risks in such circumstances.

41. The requirement to conduct a comprehensive risk assessment prior to entering into a new arrangement to provide a material service to another party, would apply to intra-group arrangements and services to non-APRA-regulated parties. An example of this for ADIs is banking as a service (BaaS), a business model whereby an ADI provides third parties access to its technology platform, allowing the third parties' customers to use the ADI's banking services. In this example, the ADI would need to conduct a risk assessment including, in particular, risks relating to money laundering, cyber-risk vulnerabilities or breaches of data confidentiality, and ensure the BaaS arrangement do not undermine its ability to meet its prudential obligations (including under the Financial Claims Scheme). An example for insurers is the provision of claims service to a third-party.

42. In assessing the materiality of the service provided, an entity would focus on whether the service exposes the entity to material operational risks or would undermine its ability to meet its prudential obligations.

Operational risk controls

29. An APRA-regulated entity must design, implement and embed internal controls to mitigate its operational risks in line with its risk appetite and meet its compliance obligations.

30. An APRA-regulated entity must regularly monitor, review and test controls for design and operating effectiveness, the frequency of which must be commensurate with the materiality of the risks being controlled. The results of testing must be reported to senior management and any gaps or deficiencies in the control environment must be rectified in a timely manner.

31. An APRA-regulated entity must remediate material weaknesses in its operational risk management, including control gaps, weaknesses and failures. This remediation must be supported by clear accountabilities and assurance and address the root causes of weaknesses in a timely manner. An APRA-regulated entity must include identified control gaps, weaknesses and failures in its operational risk profile until such matters are remediated.

43. APRA expects that any gaps, weaknesses or failures in controls are identified, escalated and rectified in a timely manner. Better practice in monitoring controls includes maintaining robust information systems, regularly assessing whether the design and operation of the controls remains effective, and re-assessing design and operating effectiveness, as well as impacts to the operational risk profile and risk appetite, when issues, incidents and breaches occur.

44. Operational risks and controls relating to business operations and critical operations may have different owners. Risk owners would have sufficient understanding of controls to ensure they are effective. Better practice is for entities to ensure that all relevant related risks and controls, whether owned by them or otherwise (including those owned by

service providers), are clearly identified, defined and recorded and have designated owners to support the assessment of control effectiveness and an accurate risk profile.

Control effectiveness

45. To assess the effectiveness of controls, better practice is to:

    a) develop criteria to ensure consistency of assessments across the entity;

    b) ensure complete capture of controls, including controls owned directly by the risk owner or by other owners, including related parties and by service providers;

    c) ensure the adequacy of coverage of controls, including preventative, detective and responsive controls;

    d) appropriately balance automated and manual controls;

    e) consider issues and incidents linked to controls, which can be indicators of weakness or gaps in the control environment;

    f) record the rationale for the control effectiveness assessment; and

    g) consider any recent changes in the environment or business strategies that could impact control effectiveness.

Control testing

46. A prudent entity would ensure controls testing programs regularly review the design and operating effectiveness of controls. It is important that entities understand the controls and the risk that they are trying to mitigate. Based on this understanding, the frequency of testing would reflect the ratings of the risks the controls are mitigating, as well as the frequency of control usage. For example, some controls may be tested quarterly, while others may be tested less frequently than annually, such as once every two years, to ensure the entity has comfort over the risk it is mitigating and that the risk is within appetite.

47. Better practice is for an entity to have controls testing that is monitored to ensure completion, with exceptions identified, escalated and remediated. Testing would typically include the objectives, scope, approach, success criteria, frequency and roles and responsibilities for testing controls. It would be conducted by staff and teams that are independent of those with operational responsibility for the controls being validated.

48. Control owners are typically responsible for ensuring that controls are regularly tested and monitored. Control gaps, weaknesses and failures would be identified as issues and managed accordingly and be reflected in the entity's operational risk profile.

Control remediation

49. Effective management action and response to address identified control weaknesses would generally include consideration of:

    a) tactical responses: temporary controls and monitoring to ensure risks are appropriately mitigated until a strategic solution is implemented; and

b) strategic solutions: changes to processes, people, and systems to improve the management of, and reduce the exposure to, operational risk on a sustainable basis.

Table 3 summarises typical approaches to management actions to remediate control weaknesses and gaps, which would be tracked in the entity's operational risk system.

Table 3. Management actions to remediate control weaknesses and gaps

Management actions to remediate control weaknesses and gaps	
Action summary	Clearly documented details of actions, including status of implementation and accountabilities for remediation
Timing	Target dates for implementation and tracking of any changes
Costs	Costs and approved budgets
Indicators	Relevant indicators for monitoring legal and regulatory compliance
Risk Profile	Control design and operating effectiveness and the extent to which risk is being mitigated is linked back to the risk profile of the entity

50. Effective root cause analysis is a key component of sound issue and control remediation. A root cause analysis can reduce the chance of the incident recurring and help to identify any common underlying weaknesses in different products and business areas, the control framework and risk culture. Root cause analysis is expected to be based on a clearly defined, documented and tested methodology that considers the role and interaction of the key elements of people, processes and systems in the entity's business operations.

Operational risk incidents

32. An APRA-regulated entity must ensure that operational risk incidents and near misses are identified, escalated, recorded and addressed in a timely manner. An APRA-regulated entity must take incidents and near misses into account in its assessment of its operational risk profile and control effectiveness in a timely manner.

33. An APRA-regulated entity must notify APRA as soon as possible, and not later than 72 hours, after becoming aware of an operational risk incident that it determines to be likely to have a material financial impact or a material impact on the ability of the entity to maintain its critical operations.

51. APRA expects that an entity would avoid extended delays or unwarranted extensions to targeted closure dates in addressing operational risk incidents. Incidents and near misses would be recorded in the entity's operational risk information system and linked to controls to ensure the risk profile accurately reflects any control weaknesses or gaps.

52. An entity would typically include mechanisms for managing all relevant stages of an incident. These typically include the steps in the table below.

Table 4. Steps in managing incidents

Managing incidents	
Detection	Detection of an incident using automated sensors and manual review
Escalation	Escalation to ensure that decision-makers are aware of the incident and to trigger response processes
Containment	Containment to minimise damage
Response	Response and remediation
Review	Post-incident analysis and review to improve incident management procedures, and support attribution and restitution (where relevant)

53. Incidents can be an important trigger for re-assessing operational risks and controls. For example, if an entity suffers a high-rated fraud incident which is deemed material, then the entity could:

    a) re-assess fraud risk in the entity's risk profile, ensuring that the inherent and residual risk ratings are correctly reflected;

    b) re-assess the controls linked to the fraud risk, including the control design and operating effectiveness to ensure they are correctly reflected;

    c) conduct a root cause analysis to assist in determining what changes are required to strengthen the control environment; and

    d) consider business process mapping to support the above.

Business continuity

34. An APRA-regulated entity must:

(a) define, identify and maintain a register of its critical operations;

(b) take reasonable steps to minimise the likelihood and impact of disruptions to its critical operations;

(c) maintain a credible BCP that sets out how it would maintain its critical operations within tolerance levels through disruptions, including disaster recovery planning for critical information assets;

(d) activate its BCP if needed in the event of a disruption; and

(e) return to normal operations promptly after a disruption is over.

54. An entity's register of critical operations would typically include:

    a) the name of the critical operation;

    b) a description of the critical operation; and

    c) tolerance levels for disruptions.

55. Business continuity is usually achieved through a combination of controls that reduce the likelihood of a business disruption and controls to reduce the impact of a disruption. This approach may include interim measures to minimise the immediate impact of a disruption, and controls to enact recovery of critical operations and contingency arrangements. Business continuity outcomes are typically better when business continuity and disaster recovery processes are aligned.

56. Better practice is for business continuity management (BCM) to be approached across the whole of the business, irrespective of organisational structures or whether an operation is performed internally or by another party.

Critical operations and tolerance levels

35. Critical operations are processes undertaken by an APRA-regulated entity or its service provider which, if disrupted beyond tolerance levels, would have a material adverse impact on its depositors, policyholders, beneficiaries or other customers, or its role in the financial system.

36. An APRA-regulated entity must, at a minimum, classify the following business operations as critical operations, unless it can justify otherwise:

(a) for an ADI: payments, deposit-taking and management, custody, settlements and clearing;

(b) for an insurer (general, life, private health): claims processing;

(c) for an RSE licensee: investment management and fund administration; and

(d) for all APRA-regulated entities: customer enquiries and the systems and infrastructure needed to support critical operations.

37. APRA may require an APRA-regulated entity, or a class of APRA-regulated entities, to classify a business operation as a critical operation.

57. Under CPS 230, it is the responsibility of an entity to identify its critical operations. Better practice would be to assess all business operations within the entity to identify which operations are critical. APRA does not expect entities to rely solely on the list of activities prescribed by APRA as critical operations.

58. In identifying critical operations, a prudent entity would consider:

    a) business operations that, if disrupted, would have a *direct* material adverse impact on depositors, policyholders, beneficiaries or other customers;

    b) business operations that, if disrupted, would have an *indirect* material adverse impact on depositors, policyholders, beneficiaries or other customers, such as through significantly impacting the entity's profitability, financial soundness, reputation or ability to comply with legal or regulatory requirements;

    c) business operations that, if disrupted, could impact the broader financial system or economy, including through flow-on effects or contagion;

    d) lessons learned from previous business disruptions and scenario analysis; and

    e) business operations that have previously been defined by the entity as critical through business impact analysis required under the superseded CPS 232.

59. APRA expects that, in identifying its critical operations, an entity would focus on outward-facing services that it needs to continue to run to support external stakeholders. The level of granularity in identifying critical operations may vary depending on the size and complexity of the entity. However, APRA expects critical operations to be defined at a level at which a meaningful tolerance level can be applied and impacts on stakeholders usefully identified and tested.

60. APRA expects that any justification by an entity that a business operation prescribed in paragraph 36 of CPS 230 is not a critical operation would be documented, approved by an Accountable Person or the equivalent at a senior management level and reviewed on at least an annual basis. APRA expects these cases would be exceptional

61. APRA expects that 'critical functions' defined for resolution planning would be classified as critical operations. Critical functions are functions an entity provides that are important to the financial system or a particular industry or community and are determined by APRA under *Prudential Standard CPS 900 Resolution Planning* (CPS 900). Not all of an entity's critical operations will be critical functions for the economy. The table below distinguishes the two concepts.

Table 5. Critical operations versus critical functions

Distinguishing concepts	Critical operations	Critical functions
Prudential standard	CPS 230	CPS 900 Resolution Planning
Definition	A process undertaken by an entity or its service provider which, if disrupted beyond tolerance levels, would have a material adverse impact on its depositors, policyholders, beneficiaries or other customers or its role in the financial system.	A function provided by an entity that is important to financial system stability or the availability of essential financial services to a particular industry or community.
Focus	Entity-level	Financial system-level
Applies to	Defined by an entity as part of BCP, and maintained at all times	Determined by APRA on a case-by-case basis

38. For each critical operation, an APRA-regulated entity must establish tolerance levels for:

(a) the maximum period of time the entity would tolerate a disruption to the operation;

(b) the maximum extent of data loss the entity would accept as a result of a disruption; and

(c) minimum service levels the entity would maintain while operating under alternative arrangements during a disruption.

39. APRA may require an APRA-regulated entity to review and change its tolerance levels for a critical operation. APRA may set tolerance levels for an APRA-regulated entity, or a class of APRA-regulated entities, where it identifies a heightened risk or material weakness.

62. Tolerance levels are akin to a risk appetite for disruption and would be clearly justified and subject to challenge and review. APRA expects that entities will set and regularly reassess tolerance levels as they learn lessons from actual disruptions, testing, and evolution in industry practices.

63. In establishing tolerance levels, better practice is to consider plausible disruption scenarios and the impact this would have on external stakeholders. For example, an ADI could consider the impact on its customers of a payment outage for a period of hours or days, and how this would affect their ability to transact and conduct their business. Similarly, an insurer could consider the example of a claims processing system outage, which would affect the insurer's ability to pay claims. For a superannuation fund, an example could be where a member is not paid their benefit due to the administrator's systems being down.

64. In setting and reviewing tolerance levels, an entity could consider:

    a) the impact on its customers and other stakeholders of a disruption;

    b) the financial or reputational impact on the entity from a prolonged or material disruption;

    c) the financial or reputational impact on the broader financial system, including any flow-on effects or contagion;

    d) any legal or regulatory requirements, including any tolerance levels set by APRA;

    e) lessons learned from previous episodes of business disruptions and scenario analysis; and

    f) recovery objectives that have previously been defined by the entity under the superseded CPS 232.

65. If a tolerance level is set too high, this would imply that the entity is willing to accept a long duration of disruption that may unduly impact its customers and in turn its own reputation, operational risk profile and prudent standing. If a tolerance level is set too low, it may not be plausible for the entity to be able to restore services within the stated limit.

66. Specific guidance on the three types of tolerance levels required in CPS 230 is outlined in the table below.

Table 6. Types of tolerance levels

Tolerances	Factors to be considered in setting tolerance levels
Maximum period of time	• Maximum allowable outages (the maximum amount of time a business service can be unavailable before the impact is deemed unacceptable). • Recovery time objectives (the maximum amount of time allowed for the recovery of information assets that relate to a business service), which is typically less than the maximum allowable outage to allow time to initiate recovery activities.
Maximum data loss	• Recovery point objective (the maximum amount of data loss that the business can tolerate in terms of time). This is typically measured by how far back the business is able to reconstruct data through other techniques such as re-keying and is normally used to inform the frequency of point-in-time backups.

Tolerances	Factors to be considered in setting tolerance levels
	• In APRA's view, sound practice is to accept that there are scenarios where data can be lost (such as a result of issues with data replication), meaning the maximum data loss should never be set at zero.
Minimum service levels	• Recovery level objective (the minimum level of service that needs to be restored to avoid impacts that are deemed unacceptable). • An entity would normally establish a recovery level objective when resumption to business-as-usual operations would require a protracted period of time. • An entity would normally determine the minimum level of people, information assets and other resources required to provide the business service.

Business continuity plan

40. An APRA-regulated entity's BCP must include:

(a) the register of critical operations and associated tolerance levels;

(b) triggers to identify a disruption and prompt activation of the plan, and arrangements to direct resources in the event of activation;

(c) actions it would take to maintain its critical operations within tolerance levels through disruptions;

(d) an assessment of the execution risks, required resources, preparatory measures, including key internal and external dependencies needed to support the effective implementation of the BCP actions; and

(e) a communications strategy to support execution of the plan.

41. An APRA-regulated entity must maintain the capabilities required to execute the BCP, including access to people, resources and technology. An APRA-regulated entity must monitor compliance with its tolerance levels and report any failure to meet tolerance levels, together with a remediation plan, to the Board.

42. An APRA-regulated entity must notify APRA as soon as possible, and not later than 24 hours after, if it has suffered a disruption to a critical operation outside tolerance. The notification must cover the nature of the disruption, the action being taken, the likely impact on the entity's business operations and the timeframe for returning to normal operations.

67. An entity's business continuity plan (BCP) caters to all stages of disruptions to critical operations: triggers and identification, initial actions (such as alternative arrangements), further actions, assessment and communications. APRA expects BCPs to be practical, concise and easy to action.

68. An entity may maintain a single or multiple BCPs. A prudent entity would maintain clear linkages between its BCP and any other management plans that deal with incidents, including disaster recovery, liquidity management and information security incident management. Common aspects where alignment is important include crisis management governance, triggers, actions and communication plans.

69. Better practice is for BCPs (including disaster recovery plans) to be sufficiently detailed so that execution does not rely on the knowledge and experience of individual staff. This reduces the key person risk when enacting the BCP and enables the rotation of staff to perform business continuity testing.

70. Where BCPs involve the use of alternative locations for the delivery of critical operations, an entity would typically ensure these alternative locations:

    a) are unlikely to be impacted by the same disruption;

    b) are accessible in a timely manner;

    c) are clearly identified within the BCPs;

    d) are usable for the duration of the disruption; and

    e) meet all legal and regulatory requirements, including security and health and safety considerations.

Testing and review

43. An APRA-regulated entity must have a systematic testing program for its BCP that covers all critical operations and includes an annual business continuity exercise. The program must test the effectiveness of the entity's BCP and its ability to meet tolerance levels in a range of severe but plausible scenarios.

44. The testing program must be tailored to the material risks of the APRA-regulated entity and include a range of severe but plausible scenarios, including disruptions to services provided by material service providers and scenarios where contingency arrangements are required. APRA may require the inclusion of an APRA-determined scenario in a business continuity exercise for an APRA regulated entity, or a class of APRA-regulated entities.

45. An APRA-regulated entity must update, as necessary, its BCP on an annual basis to reflect any changes in legal or organisational structure, business mix, strategy or risk profile or for shortcomings identified as a result of the review and testing of the BCP.

71. Systematic testing of BCPs and associated disaster recovery plans (BCP tests) would typically occur on a cycle to ensure all critical operations are covered over a specified multi-year timeframe (for example, three years). There is no expectation that all severe but plausible scenarios are tested every year, but specific test frequency and rigour should ideally be commensurate with the impact of the plausible disruption scenarios.

72. The aims of testing are to highlight any deficiencies, build experience in managing a crisis and proactively strengthen the BCP, and ultimately ensure an entity is prepared should an actual disruption occur. When designing the testing program, an entity could consider:

    a) the involvement of business users;

    b) the rotation of staff executing tests in order to reduce the reliance on key personnel;

c) the involvement of independent observers (e.g. risk or internal audit) to identify any areas for improvement; and in relation to service provider arrangements, the potential for joint testing.

73. An entity would usually consider the use of simulation techniques and testing in environments isolated from production, to ensure business is not disrupted. It is important that controls are in place to ensure that information security is not compromised throughout the testing process.

74. It is important that success criteria for BCP tests are clearly defined, including the circumstances under which re-testing would be required. Test results and the execution of any findings such as remediation would be reported to and reviewed by the Board, with associated follow-up actions formally tracked and reported.

75. Reports on BCP tests would typically include:

a) the scope, including the critical operations included (and excluded) and the specific tolerance levels tested;

b) what was demonstrated by the test, including whether tolerance levels were met; and

c) any issues raised, root causes and required remediation, including timeframes and accountabilities for actions.

76. Entities that rely on service providers should seek evidence of the periodic testing of BCPs and relevant arrangements by those service providers.

77. In undertaking the review and update of BCPs, better practice is to take into account the results of testing, internal audit findings, and any lessons learned from actual business disruptions.

78. A prudent entity would review and update its BCP as soon as possible following a material change in its structure, business or risk profile, such as after a merger or acquisition or a major external shock.

79. The use of contingency arrangements (where viable options exist) enables entities to better avoid a reactionary approach to responding to a disruption where recovery plans do not operate as intended, including those of service providers and related parties.

46. An APRA-regulated entity's internal audit function must periodically review the entity's BCP and provide assurance to the Board that the BCP sets out a credible plan for how the entity would maintain its critical operations within tolerance levels through severe disruptions and that testing procedures are adequate and have been conducted satisfactorily.

80. Internal audit is an important vehicle for assurance. The Board could also consider seeking assurance through expert opinion or other means to complement internal audit. This would typically occur where the required skills do not reside within internal audit or the area subject to audit pertains to service providers.

81. An audit program would typically assess all aspects of business continuity capability over time. Additional assurance projects could be triggered by changes to services, processes, information assets, the business environment and stakeholder expectations.

82. Where internal audit relies on control testing performed by other areas of the business, it would ideally assess the scope and quality of the testing conducted in order to determine how much reliance can be placed on it.

Management of service provider arrangements

47. An APRA-regulated entity must maintain a comprehensive service provider management policy. The policy must cover how the entity will identify material service providers and manage service provider arrangements, including the management of material risks associated with the arrangements.

48. The policy must include:

(a) the entity's approach to entering into, monitoring, substituting and exiting agreements with material service providers;

(b) the entity's approach to managing the risks associated with material service providers; and

(c) the entity's approach to managing the risks associated with any fourth parties that material service providers rely on to deliver a critical operation to the APRA-regulated entity.

83. Where an entity uses a service provider the entity remains responsible for owning and managing its risk and, as a result, is expected to have visibility of the controls and their effectiveness where the service provider manages the controls on behalf of the entity.

84. Common areas addressed by a service provider management policy would typically include:

    a) roles and responsibilities of accountable persons or the equivalent;

    b) processes for the selection of and due diligence on service providers;

    c) management of risks associated with service providers;

    d) methodology for the assessment of the materiality of service providers;

    e) on-boarding and exiting procedures;

    f) BCPs and alternative arrangement considerations (including where the service provider is unable to provide the service for an extended period of time);

    g) issue management and escalation procedures;

    h) processes for vetting key personnel of service providers; and

    i) oversight processes and practices to monitor the service providers, service level agreements, and risks.

85. While CPS 230 outlines requirements for the management of material service providers, an entity's service provider management policy would normally include expectations of how *all* service provider arrangements are to be managed.

86. An entity would typically periodically evaluate the effectiveness of its service provider management policy in practice. This evaluation could be conducted through a review of the performance of service providers, the results of audits, and other independent reviews.

87. APRA expects that an entity would be able to demonstrate its understanding and management of risks at all stages of a material service provider arrangement, from strategic planning and service provider selection through to the management of and exiting the arrangement.

88. Better practice for ongoing oversight of service providers would be for an entity to ensure the service provider's internal operational risk framework is sound and operates effectively; in particular, the service provider would be able to demonstrate the prudent identification and management of risks, controls, obligations, incidents and issues.

89. Accordingly, APRA expects that a prudent entity would have visibility of risk management practices of the service provider and take reasonable steps to ensure consistent standards are maintained that would not fall below those it would use if the service was maintained internally. This includes consistent process mapping for all services, whether maintained by the entity or a service provider, verified through practices such as onsite visits and control monitoring.

90. Service providers may, in turn, rely on other service providers (fourth parties). Fourth party providers may in turn rely on other service providers. This can result in an entity relying on downstream service providers without direct agreements with these providers, which can impede the ability of the entity to manage risks in its supply chain.

91. APRA expects that an entity would be aware of, and manage, the risks associated with fourth party and other downstream service providers for critical operations, including the correlated risk that arises when several of its service providers are reliant on the same fourth party. This would typically, at a minimum, include:

    a) due diligence to identify material fourth parties and, where feasible, other downstream providers that could materially impact the performance of the service;

    b) contractual provisions between the entity and the material service provider to ensure the entity is informed of material fourth parties; and

    c) assurance from service providers that they have the capability to manage material fourth parties.

92. Better practice would be for an entity to ensure that service providers undertake appropriate monitoring of risks managed by fourth parties. This would typically extend to monitoring key factors, including control environment health and incident management. Monitoring could include regular reporting to the regulated entity from the service provider on operational performance and risk management.

Material service providers

49. An APRA-regulated entity must identify and maintain a register of its material service providers and manage the material risks associated with using these providers. Material service providers are those on which the entity relies to undertake a critical operation or that expose it to material operational risk. Material arrangements are those on which the entity relies to undertake a critical operation or that expose it to material operational risk.

50. An APRA-regulated entity must, at a minimum, classify a provider of the following services as material service provider, unless it can justify otherwise:

(a) for an ADI: credit assessment, funding and liquidity management and mortgage brokerage;

(b) for an insurer (general, life, private health): underwriting, claims management, insurance brokerage and reinsurance;

(c) for an RSE licensee: fund administration, custodial services, investment management and arrangements with promoters and financial planners; and

(d) for all APRA-regulated entities: risk management, core technology services and internal audit.

93. APRA does not expect entities to rely solely on the list of services prescribed by APRA as material service providers. APRA expects that a prudent entity would assess all service providers within the entity with clear criteria for identifying which are material, based on the definition in CPS 230.

94. In determining which service providers are material, an entity would consider:

    a) whether the service supports a critical business operation;

    b) the totality of services provided by the service provider;

    c) the nature of the services provided and whether it exposes the entity to material operational risk, including for example cyber risks or mis-selling risks, or in the event the service or service provider is compromised (operationally, financially or reputationally);

    d) the degree of difficulty in exiting the arrangement and transitioning delivery of services to another service provider or bringing it in-house; and

    e) whether the service involves sensitive or critical information assets, as classified by the entity for the purposes of CPS 234, including for example the consequence of a data breach.

95. Better practice is for the register to contain all service providers and services, with material providers clearly identified.

96. A prudent entity would manage the operational risk associated with cohorts of service providers, where the aggregate impact of those service providers is material, but each individual provider is not.

97. APRA expects that any justification by an entity not to classify a service provider prescribed by APRA as material would be documented, approved by an Accountable Person or the equivalent at a senior management level, and reviewed on at least an annual basis.

51. An APRA-regulated entity must submit its register of material service providers to APRA on an annual basis.

52. APRA may require an APRA-regulated entity, or a class of APRA-regulated entities, to classify a service provider, type of service provider or service provider arrangement as material.

Service provider agreements

53. Before entering into or materially modifying a material arrangement, an APRA-regulated entity must:

(a) undertake appropriate due diligence, including an appropriate selection process and an assessment of the ability of the service provider to provide the service on an ongoing basis; and

(b) assess the financial and non-financial risks from reliance on the service provider, including risks associated with geographic location or concentration of the service provider(s) or parties the service provider relies upon in providing the service.

98. CPS 230 requires entities to identify material service providers, and to maintain formal agreements for material arrangements with these providers. Not all arrangements with a material service provider will be material to the entity.

99. When selecting and assessing a service provider for material arrangements, an entity would typically consider the following against its risk appetite:

    a) business services and capabilities which must be retained in-house;

    b) country or region risk;

    c) supplier risk;

    d) concentration risk; and

    e) reputational risk.

100. APRA expects an entity to adopt a measured approach when considering services, particularly those which are delivered from another jurisdiction. It is important that the entity is fully aware of the risks involved in engaging a service provider in another jurisdiction, including undertaking an assessment of whether the additional risks are within risk appetite. This would include consideration of:

    a) the ability to continue operations and meet core obligations following a loss of service;

    b) maintenance of information security;

c) the ability to own and manage controls on its behalf;

d) compliance with legislative and prudential requirements; and

e) impediments, both legal and technical, to APRA being able to fulfil its duties as prudential regulator, including timely access to information in a usable form.

54. For all material arrangements, an APRA-regulated entity must maintain a formal legally binding agreement (formal agreement). The formal agreement must, at a minimum:

(a) specify the services covered by the agreement and associated service levels;

(b) set out the rights, responsibilities and expectations of each party to the agreement, including in relation to the ownership of assets, ownership and control of data, dispute resolution, audit access, liability and indemnity;

(c) include provisions to ensure the ability of the entity to meet its legal and compliance obligations;

(d) require notification 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;

(e) require the liability for any failure on the part of any sub-contractor to be the responsibility of the service provider;

(f) include a force majeure provision indicating those parts of the contract that would continue in the case of a force majeure event; and

(g) termination provisions including, but not limited to, the right to terminate both the arrangement in its entirety or parts of the arrangement. For an RSE licensee, termination provisions must include the ability for the RSE licensee to terminate the arrangement where to continue the arrangement would be inconsistent with the RSE licensee's duty to act in the best financial interests of beneficiaries (refer to subsection 52(2)(c) of the SIS Act).

101. The formal legally binding agreement required under CPS 230 would typically be sufficiently flexible to accommodate changes.

102. Service levels and performance are typically documented via a service-level agreement. This would normally specify the metrics by which the service provider is measured and monitored.

103. The agreement would typically specify the extent of liability of each party and, in particular, whether liability for negligence is limited. The agreement would usually specify any indemnities and provide details of any associated insurance arrangements. Also, consideration would normally be given to the extent of liability to both the entity and service provider in relation to the use of other service providers.

104. Termination provisions would typically detail transition arrangements as well as ownership and access to documents, data, intellectual property and other assets. Termination provisions would also typically specify the time period for which the services would continue to be provided.

55. The formal agreement must also include provisions that:

(a) allow APRA access to documentation, data and any other information related to the provision of the service;

(b) allow APRA the right to conduct an on-site visit to the service provider; and

(c) ensure the service provider agrees not to impede APRA in fulfilling its duties as prudential regulator.

105. If APRA intends to seek information directly from a service provider, or undertake an on-site visit to a service provider, it will typically inform the entity in advance of its intention to do so.

56. For each material arrangement, an APRA-regulated entity must:

(a) identify and manage risks that could affect the ability of the service provider to provide the service on an ongoing basis;

(b) identify and manage risks to the APRA-regulated entity that could result from the arrangement, such as step-in risk or contagion risk;

(c) ensure it can execute its BCP if needed; and

(d) ensure it can conduct an orderly exit from the arrangement if needed.

57. APRA may require an APRA-regulated entity to review and make changes to a service provider arrangement where it identifies heightened prudential concerns.

Monitoring, notifications and review

58. An APRA-regulated entity must monitor and ensure that senior management receive reporting on material arrangements commensurate with the nature and usage of the service. This monitoring must include a regular assessment of:

(a) performance under the service agreement with reference to agreed service levels;

(b) the effectiveness of controls to manage the risks associated with the use of the service provider; and

(c) compliance of both parties with the service provider agreement.

106. Monitoring typically entails the regular review of key information and regular engagement with a service provider. Better practice is to monitor:

a) performance against agreed service levels and other expectations;

b) the control environment, business continuity capabilities and information security capabilities;

c) key changes, including service delivery location, key personnel, use of service providers and the control environment;

d) disruptions and operational risk incidents;

e) issues and emerging risks; and

f) the ongoing viability (financial and non-financial) of the service provider and the services delivered, including strategic plans and investment in the service;

107. The assessment of controls to manage the risks associated with the use of service providers could include a combination of formal reporting, interviews, surveys, testing, certifications, contractual reviews, attestations and independent assurance assessments. Weaknesses identified should be monitored by the entity to ensure that they are addressed in a timely manner by the service provider.

108. An entity would normally undertake periodic reviews of the arrangement with a service provider. The review would typically assess performance against the agreement, any operational issues that have occurred (including information security incidents and service disruptions), control effectiveness, information security capabilities and business continuity capabilities, any changes to the strategic direction of the service provider or service, and comparisons to other offerings within the market. Typically, the results of the review would be communicated to the service provider, including what is working well and what aspects of the agreement warrant attention.

59. An APRA-regulated entity must notify APRA:

(a) 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

(b) 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.

60. An APRA-regulated entity's internal audit function must review any proposed outsourcing of a critical operation. The internal audit function must regularly report to the Board or Board Audit Committee on compliance of such arrangements with the entity's service provider management policy.

DRAFT

APRA