Prudential Standard CPS 230

Operational Risk Management

Objectives and key requirements of this Prudential Standard

The aim of this Prudential Standard is to ensure that an APRA-regulated entity is resilient to operational risks and disruptions. An APRA-regulated entity must effectively manage its operational risks, maintain its critical operations through disruptions, and manage the risks arising from service providers.

An APRA-regulated entity's approach to operational risk must be appropriate to its size, business mix and complexity. The key requirements of this Prudential Standard are that an APRA-regulated entity must:

- identify, assess and manage its operational risks, with effective internal controls, monitoring and remediation;
- be able to continue to deliver its critical operations within tolerance levels through severe disruptions, with a credible business continuity plan (BCP); and
- effectively manage the risks associated with service providers, with a comprehensive service provider management policy, formal agreements and robust monitoring.

Authority

1. This Prudential Standard is made under:

   (a) section 11AF of the *Banking Act 1959* (Banking Act);

   (b) section 32 of the *Insurance Act 1973* (Insurance Act);

   (c) section 230A of the *Life Insurance Act 1995* (Life Insurance Act);

   (d) section 92 of the *Private Health Insurance (Prudential Supervision) Act 2015* (PHIPS Act); and

   (e) section 34C of the *Superannuation Industry (Supervision) Act 1993* (SIS Act).

Application and commencement

2. This Prudential Standard applies to all APRA-regulated entities defined as:

   (a) **authorised deposit-taking institutions** (**ADIs**), including **foreign ADIs**, and **non-operating holding companies** authorised under the Banking Act (authorised banking NOHCs);

   (b) **general insurers**, including **Category C insurers**, non-operating holding companies authorised under the Insurance Act (authorised insurance NOHCs), and **parent entities** of **Level 2 insurance groups**;

   (c) **life companies**, including **friendly societies**, **eligible foreign life insurance companies** (EFLICs) and non-operating holding companies registered under the Life Insurance Act (registered life NOHCs);

   (d) **private health insurers** registered under the PHIPS Act; and

   (e) registrable superannuation entity licensees (**RSE licensees)** under the SIS Act in respect of their business operations.[1]

3. The obligations imposed by this Prudential Standard on, or in relation to, a foreign ADI, a Category C insurer and an EFLIC apply only in relation to the Australian branch operations of that entity.

4. Where an APRA-regulated entity is the Head of a group,[2] it must comply with a requirement of this Prudential Standard:

---

1 RSE licensee has the meaning given in subsection 10(1) of the SIS Act. For the purposes of this Prudential Standard, an RSE licensee's business operations includes all activities of an RSE licensee, including the activities of each RSE of which it is the licensee, and all other activities of the RSE licensee to the extent that they are relevant to, or may impact on, its activities as an RSE licensee.

2 Where a Level 2 group operates within a Level 3 group, a requirement expressed as applying to a Head of a group is to be read as applying to the Level 3 Head.

(a) in its capacity as an APRA-regulated entity;

(b) by ensuring that the requirement is applied appropriately throughout the group,[3] including in relation to entities that are not APRA-regulated; and

(c) on a group basis.

5. In applying the requirements of this Prudential Standard on a group basis, references to an APRA-regulated entity are to be read as 'Head of a group' and references to entity are to be read as group.

6. This Prudential Standard commences on 1 January 2024.

Interpretation

7. Terms that are defined in *Prudential Standard APS 001 Definitions*, *Prudential Standard GPS 001 Definitions*, *Prudential Standard LPS 001 Definitions*, *Prudential Standard HPS 001 Definitions* or *Prudential Standard 3PS 001 Definitions* appear in bold the first time they are used in this Prudential Standard.

8. In this Prudential Standard, unless the contrary intention appears, a reference to an Act, Regulation or Prudential Standard is a reference to the Act, Regulation or Prudential Standard as in force from time to time.

9. Where this Prudential Standard provides for APRA to exercise a power or discretion, the power or discretion is to be exercised in writing.

Adjustments and exclusions

10. APRA may adjust or exclude a specific prudential requirement in this Prudential Standard in relation to an APRA-regulated entity.[4]

Key principles

11. 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

---

[3] Group means a Level 2 group, Level 3 group or a group comprising the RSE licensee and all connected entities (as defined in subsection 10(1) of the SIS Act) and all related bodies corporate (with the meaning given in section 50 of the *Corporations Act 2001*) of the RSE licensee, as relevant. Level 2 group means the entities that comprise Level 2 (for ADIs) or Level 2 insurance groups (for general insurers). For the avoidance of doubt, group includes a group as defined in APS 001 and, for an RSE licensee, where the RSE licensee is part of a corporate group.

[4] Refer to subsection 11AF(2) of the Banking Act, subsection 32(3D) of the Insurance Act, subsection 230A(4) of the Life Insurance Act, subsection 92(4) of the PHIPS Act and subsection 34C(5) of the SIS Act.

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

12. 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.

13. 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 after a disruption is over.

14. 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.

Risk management framework

15. 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 and limits;

(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.

16. 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.[5] The reviews must cover the aspects of operational risk management set out in paragraph 15.

17. 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 financial contingency planning.

---

5 Refer to CPS 220 and SPS 220 for the requirement to undertake a review of the risk management framework.

18. Where APRA considers 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;[6]

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

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

Role of the Board

19. The **Board** of an APRA-regulated entity is ultimately accountable for the oversight of an entity's operational risk management, including business continuity and the management of service provider arrangements.[7]

20. The Board must ensure that the APRA-regulated entity sets clear roles and responsibilities for **senior managers**[8] for operational risk management, including business continuity and the management of service provider arrangements.

21. 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 oversee the execution of any findings; and

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

22. Senior management of an APRA-regulated entity must provide clear and comprehensive 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.

---

6 For an RSE licensee, APRA may require an RSE licensee to meet an ORFR target amount determined by APRA under *Prudential Standard SPS 114 Operational Risk Financial Requirement*.

7 For an RSE licensee, a reference to the Board is to be read as a reference to the Board of directors or group of individual trustees of an RSE licensee, as applicable. 'Group of individual trustees' has the meaning given in subsection 10(1) of the SIS Act. A reference to the Board in the case of a foreign ADI is a reference to the senior officer outside Australia.

8 Senior manager in relation to life insurers has the meaning given in the Life Insurance Act, and in relation to RSE licensees has the meaning given in *Prudential Standard SPS 520 Fit and Proper*.

Operational risk management

23. 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, reputational risk and change management risk. Senior management are responsible for operational risk management across the end-to-end process for all business operations.

24. An APRA-regulated entity must maintain appropriate and sound information and information technology (IT) infrastructure 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 IT infrastructure and meet the requirements for information security in *Prudential Standard CPS 234 Information Security* (CPS 234).

Operational risk profile and assessment

25. 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.[9] This must include an assessment of the impact of new products, services, geographies and technologies on its operational risk profile.

26. 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.

27. An APRA-regulated entity must conduct a comprehensive risk assessment before providing a material service to another party to ensure that it 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.

---

[9] Refer to *Prudential Standard SPS 515 Strategic Planning and Member Outcomes* for requirements applying to an RSE licensee with respect to strategic objectives and business planning.

Operational risk controls

28. 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.

29. 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.

30. 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.

Operational risk incidents

31. 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.

32. 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.[10]

Business continuity

33. 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;[11]

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

---

[10] A notification of an information security incident reported under CPS 234 does not need to be separately reported under the notification requirements of this Prudential Standard.

[11] An entity may have a number of BCPs. A BCP may include separate crisis management plans and disaster recovery plans.

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

Critical operations and tolerance levels

34. 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.

35. For the purposes of this Prudential Standard, critical operations include, but are not limited to: payments, deposit-taking and management, custody, settlements, clearing, claims processing, investment management, fund administration, customer enquiries and the systems and infrastructure needed to support these operations.

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

37. For each critical operation, an APRA-regulated entity must establish Board-approved 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.

38. 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.

Business continuity plan

39. 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.

40. An APRA-regulated entity must maintain the capabilities required to execute the BCP, including access to people, resources and technology.[12] 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.

41. An APRA-regulated entity must notify APRA as soon as possible, and no later than 24 hours, if it has activated its BCP. 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.

Testing and review

42. 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.

43. 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.

44. An APRA-regulated entity must review and 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.

45. 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.

Management of service provider arrangements

46. An APRA-regulated entity must maintain a comprehensive service provider management policy that sets out how it will identify material service providers and manage the arrangements with such providers, including the management of material risks associated with the arrangements.

47. The policy must include:

    (a) a register of the entity's material service providers;

[12] Capabilities required to execute the BCP may be maintained within the APRA-regulated entity or via an agreement with another party. For the avoidance of doubt, such agreements with other parties must meet the requirements for management of service providers arrangements in this Prudential Standard.

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

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

(d) the entity's approach to managing the risks associated with any fourth parties that material service providers rely on.[13]

Material service providers

48. 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.[14]

49. Material service providers include, but are not limited to, those that provide the following services to an APRA-regulated entity: risk management, core technology services, internal audit, credit assessment, funding and liquidity management, mortgage brokerage, underwriting, claims management, insurance brokerage, reinsurance, fund administration, custodial services, investment management and arrangements with promoters and financial planners.

50. Material service providers also include providers that manage information assets classified as critical or sensitive under CPS 234.

51. An APRA-regulated entity must submit its register of material service providers to APRA on an annual basis. APRA may require an APRA-regulated entity, or a class of APRA-regulated entities, to classify a service provider, or type of service provider, as material.

Service provider agreements

52. Before entering into, renewing or materially modifying an arrangement with a material service provider, an APRA-regulated entity must:

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

(b) assess the financial and non-financial risks from reliance on a particular 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; and

---

13 A fourth party is a party that a service provider relies on in delivering services to an APRA-regulated entity.

14 A material service provider may be a third party, related party or connected entity. A service provider may be identified as material as a result of an individual arrangement or multiple arrangements with an APRA-regulated entity.

(c) take reasonable steps to assess whether the provider is systemically important in Australia.

53. For all material service provider arrangements, an APRA-regulated entity must maintain a formal legally binding 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, 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 section 52(2)(c) of the SIS Act).

54. 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.

55. For each arrangement with a material service provider, an APRA-regulated entity must:

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

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

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

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

56. 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

57. An APRA-regulated entity must monitor and report to senior management on material service provider 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.

58. 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 offshoring[15] agreement with a material service provider, or when there is a significant change proposed to the agreement, including in circumstances where data or personnel relevant to the service being provided will be located offshore.

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

[15] Offshoring means an arrangement with a material service provider where the service provided is undertaken outside Australia. Offshoring includes arrangements where the service provider is incorporated in Australia, but the physical location of the service being provided is undertaken outside Australia. Offshoring does not include arrangements where the physical location of a service is performed within Australia but the service provider is not incorporated in Australia.