

**Banking, Insurance, Life Insurance, Health Insurance and Superannuation (prudential standard) determination No. 2 of 2023**

**EXPLANATORY STATEMENT**

**Prepared by the Australian Prudential Regulation Authority (APRA)**

*Banking Act 1959*, section 11AF

*Insurance Act 1973*, section 32

*Life Insurance Act 1995*, section 230A

*Private Health Insurance (Prudential Supervision) Act 2015*, section 92

*Superannuation Industry (Supervision) Act 1993*, section 34C

APRA may, in writing, determine a prudential standard that applies to an APRA-regulated entity under:

- (1) subsection 11AF(1) of the *Banking Act 1959* (Banking Act), which applies to all authorised deposit-taking institutions (ADIs), authorised banking non-operating holding companies (authorised banking NOHCs) and subsidiaries of ADIs and authorised banking NOHCs;
- (2) subsection 32(1) of the *Insurance Act 1973* (Insurance Act), which applies to all general insurers and authorised non-operating holding companies (authorised insurance NOHCs), and subsidiaries of general insurers and authorised insurance NOHCs;
- (3) subsection 230A(1) of the *Life Insurance Act 1995* (Life Insurance Act), which applies to all life companies, including friendly societies and registered life non-operating holding companies (registered life NOHCs), and subsidiaries of life companies and registered life NOHCs;
- (4) subsections 92(1) of the *Private Health Insurance (Prudential Supervision) Act 2015* (PHIPS Act), which applies to all private health insurers; and
- (5) subsection 34C(1) of the *Superannuation Industry (Supervision) Act 1993* (SIS Act), which applies to all registered superannuation entity licensees (RSE licensees) and connected entities of RSE licensees.

APRA may, in writing, vary or revoke a prudential standard that applies to an APRA-regulated institution under:

- (1) subsection 11AF(3) of the Banking Act, which applies to all ADIs, authorised banking NOHCs and subsidiaries of ADIs and authorised banking NOHCs;

- (2) subsection 32(4) of the Insurance Act, which applies to all general insurers and authorised insurance NOHCs, and subsidiaries of general insurers and authorised insurance NOHCs;
- (3) subsection 230A(5) of the Life Insurance Act, which applies to all life companies, including friendly societies and registered life NOHCs, and subsidiaries of life companies and registered life NOHCs;
- (4) under subsection 92(5) of the PHIPS Act, which applies to all private health insurers; and
- (5) subsection 34C(6) of the SIS Act, which applies to all RSE licensees and connected entities of RSE licensees.

On 11 September 2023, APRA made Banking, Insurance, Life Insurance, Health Insurance and Superannuation (prudential standard) determination No. 2 of 2023 (the instrument) which revokes:

- (1) *Prudential Standard CPS 231 Outsourcing* ;
- (2) *Prudential Standard CPS 232 Business Continuity Management*;
- (3) *Prudential Standard SPS 231 Outsourcing*;
- (4) *Prudential Standard SPS 232 Business Continuity Management*; and
- (5) *Prudential Standard HPS 231 Outsourcing*

(together, the existing prudential standards)

and determines *Prudential Standard CPS 230 Operational Risk Management (CPS 230)*.

The instrument commences on 1 July 2025.

## **1. Background**

APRA's mandate is to ensure the safety and soundness of prudentially regulated financial institutions so that they can meet their financial promises to depositors, policyholders and fund members within a stable, efficient and competitive financial system.

APRA carries out this mandate through a multi-layered prudential framework that encompasses licensing and supervision of entities. The Banking Act, Insurance Act, Life Insurance Act, PHIPS Act and SIS Act allow APRA to issue legally binding prudential standards that set out specific prudential requirements with which APRA-regulated entities must comply.

APRA regularly reviews its regulatory regime and amends its prudential requirements as a result of a number of factors, including:

- international developments;
- changes in financial market conditions or changes in risk management practices, in response to identified weaknesses in the prudential framework; and

- to reduce potential negative impacts of emerging industry issues.

A resilient financial system requires strong operational risk management, which is fundamental to financial safety of APRA-regulated entities and financial system stability. CPS 230 sets out requirements to ensure that APRA-regulated entities maintain operational risk management arrangements that ensure operational risks are appropriately managed through effective controls, monitoring and remediation; that entities are prepared to respond to disruptions and maintain critical operations through disruptions; and risks arising from the use of service providers are managed appropriately.

With the commencement of CPS 230 on 1 July 2025, the existing prudential standards will be revoked as CPS 230 will incorporate updated coverage of APRA's requirements for service provision (including outsourcing) and business continuity management.

## **2. Purpose and operation of the instruments**

The purpose of the instrument is to revoke existing prudential standards for outsourcing and business continuity management and determine a new prudential standard, CPS 230.

CPS 230 is designed to:

- strengthen the operational risk management of APRA-regulated entities;
- improve business continuity planning to ensure APRA-regulated entities can effectively respond to severe business disruptions and maintain critical operations and minimise material adverse impacts on depositors, policyholders, beneficiaries or other customers or an entity's role in the financial system; and
- strengthen the management of third parties whom the regulated entity relies upon in providing critical operations.

### ***Explanation of specific provisions in CPS 230***

#### *Authority (paragraph 1)*

This paragraph outlines the legislative provisions under which CPS 230 is made.

#### *Application and commencement (paragraphs 2-7)*

Paragraph 2 sets out details of the APRA-regulated entities that CPS 230 applies to.

Paragraph 6 sets out the commencement date of the standard.

Paragraph 7 provides transition arrangements in relation to pre-existing contractual arrangements with a service provider as at the date of commencement of CPS 230.

#### *Interpretation (paragraphs 8-10)*

Paragraph 8 outlines that words which appear in bold the first time they are used in CPS 230 are defined in APRA's Definitions prudential standards.

Paragraph 9 acknowledges that unless a contrary intention appears, references to an Act, Regulation or Prudential Standard are references incorporated as in force from time to time.

Paragraph 10 requires that where APRA exercises a power or discretion provided for under CPS 230, APRA will do so in writing.

#### *Adjustments and exclusions (paragraph 11)*

Paragraph 11 gives APRA the power to adjust or exclude a specific prudential requirement within CPS 230 in relation to an APRA-regulated entity. The relevant legislative provisions that give effect to APRA's exercise of such a power are noted in the accompanying footnote 4.

#### *Key principles (paragraphs 12-15)*

Paragraphs 12-15 set out the key principles that an APRA-regulated entity is to have regard to in the management of its operational risk, business continuity planning and management of service provider arrangements.

Paragraph 12 lays out general principles that underpin the specific requirements on operational risk management set out in the remainder of CPS 230.

Paragraph 13 requires an APRA-regulated entity to identify, assess and manage the operational risks that arise from its activities.

Paragraph 14 requires an APRA-regulated entity to take steps to prevent disruption to its critical operations as well as building in resilience to these operations, so that the entity can continue to operate should a disruption occur, and that the entity returns to normal operations as expeditiously as possible.

Paragraph 15 requires that an APRA-regulated entity must not enter into an arrangement with a service provider if the arrangement prevents the regulated entity from meeting its prudential obligations. When an APRA-regulated entity enters into an arrangement with a service provider, it must identify the risks associated with placing reliance on a service provider and continue to manage all such risks for the life of the arrangement.

#### *Risk management framework (paragraphs 16-19)*

The purpose of this section is to ensure that an APRA-regulated entity approaches operational risk management in the context of its broader risk management planning, rather than looking at operational risk management in isolation.

Paragraphs 16 and 17 set out specific requirements an APRA-regulated entity is to implement in order to comply with CPS 230 in the context of the entity's broader risk management framework required under *Prudential Standard CPS 220 Risk Management* and *Prudential Standard SPS 220 Risk Management*.

Paragraph 18 requires an APRA-regulated entity to integrate operational risk management in its overall risk management framework and ensure that business continuity planning is consistent with APRA's prudential requirements on recovery and exit planning as set out in *Prudential Standard CPS 190 Recovery and exit planning*.

Paragraph 19 notes actions APRA may take if APRA considers that there are material weaknesses with an APRA-regulated entity's approach to, and management of, operational risk management. These actions reflect existing powers APRA has the discretion to use for prudential purposes.

#### *Role and responsibilities (paragraphs 20-23)*

Paragraph 20 provides that the Board is ultimately accountable for oversight of an APRA-regulated entity's operational risk management, as well as business continuity and the management of service provider arrangements.

Paragraph 21 requires the Board to ensure there is clarity within an APRA-regulated entity as to the roles and responsibilities of senior managers in the context of operational risk management, including business continuity management and the management of service provider arrangements.

Paragraph 22 sets out APRA's requirements as to what the Board must do in discharging its role in overseeing operational risk management. This includes the Board: overseeing operational risk management, including the effectiveness of controls in maintaining the entity's risk profile within risk appetite; approving the business continuity plan and tolerance levels for disruptions to critical operations and reviewing the results of testing; and approving the entity's service provider management policy and reviewing risk and performance reporting on material service providers.

Paragraph 23 imposes an obligation on senior management of an APRA-regulated entity to ensure that when the Board is making decisions that could affect the resilience of critical operations (as defined in paragraph 35), the Board is provided with clear and comprehensive information on the expected impacts on the regulated entity's critical operations.

#### *Operational risk management (paragraphs 24-33)*

Paragraph 24 requires an APRA-regulated entity to manage all its operational risks, which include legal risk, regulatory risk, compliance risk, conduct risk, technology risk, data risk and change management risk. Senior management are responsible for operational risk management for all business operations.

Paragraph 25 requires an APRA-regulated entity to maintain its information and information technology capability in order to meet its business requirements and to support both its critical operations and risk management. In managing technology risks, an APRA-regulated entity must monitor its information assets and meet the requirements for information security in *Prudential Standard CPS 234 Information Security*.

Paragraph 26 requires an APRA-regulated entity to assess the impact of strategic decision-making on both its operational risk profile and operational resilience. This includes an assessment of the impact of new products, services, geographies and technologies on the entity's operational risk profile.

Paragraph 27 sets out requirements an APRA-regulated entity must meet in maintaining its operational risk profile. These include maintaining information systems, documents processes and resources required to deliver critical operations and undertaking scenarios analysis to identify and assess the impacts of severe operational risk events.

Paragraph 28 requires an APRA-regulated entity to undertake a comprehensive risk assessment before it provides a material service to another party. This is in the case where an APRA-regulated entity is itself the party that will be providing the service. An APRA-regulated entity providing such a service must be able to continue to meet its prudential obligations in full.

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

Paragraph 30 requires an APRA-regulated entity to maintain its controls through regular monitoring, review and testing to ensure their ongoing effectiveness, report the results to senior management and rectify any gaps or deficiencies in the control environment promptly.

Paragraph 31 requires an APRA-regulated entity to remediate material weaknesses in its operational risk management. There must be clear accountability for remediation work required and identified gaps, weaknesses and failures must themselves be included in the entity's operational risk profile until such time as they are remediated.

Paragraph 32 requires an APRA-regulated entity to have a process for the identification, escalation, recording and rectification of operational risk incidents and near misses. Such incidents and near misses must be accounted for in the entity's operational risk profile and taken into account in its control effectiveness.

Paragraph 33 requires an APRA-regulated entity to notify APRA on becoming aware of an operational risk incident that could have either a material financial impact or a material impact on the regulated entity's critical operations. Notification must be made as soon as possible, and in any event not more than 72 hours after the entity becomes aware of the incident.

#### *Business continuity (paragraphs 34-46)*

Paragraph 34 sets out actions an APRA-regulated entity must take in relation to its critical operations, including: maintaining a register of critical operations; taking reasonable steps to minimise the likelihood and impact of disruptions to critical operations; maintaining a business continuity plan that details how the entity would maintain its critical operations

during a disruption; activating its business continuity plan in the event of a disruption; and returning to normal operations promptly after a disruption.

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

Paragraph 36 prescribes certain business operations as critical operations for the purposes of CPS 230. This paragraph allows a regulated entity to not classify a prescribed business operation as a critical operation provided it can justify its decision to do so.

Paragraph 37 allows APRA to direct a regulated entity to classify a business operation as a critical operation.

Paragraph 38 requires an APRA-regulated entity to set tolerance levels in relation to each critical operation. Tolerance levels indicate the entity's appetite for the impact of a disruption on a critical operation in relation to matters including the period of the disruption, data loss and minimum service levels to be maintained during a disruption.

Paragraph 39 gives APRA discretion to direct an APRA-regulated entity to change its tolerance levels and for APRA to set tolerance levels should APRA identify heightened risk or material weakness within the APRA-regulated entity.

Paragraph 40 sets out matters that an APRA-regulated entity must include as part of its business continuity plan.

Paragraph 41 requires an APRA-regulated entity to maintain the capabilities to be able to execute its business continuity plan. This includes necessary people, resources and technology. This provision also requires the regulated entity to monitor compliance with tolerance levels for critical operations and to notify any failure to meet tolerance levels to the Board, along with a remediation plan.

Paragraph 42 is a notification requirement. An APRA-regulated entity must notify APRA as soon as possible, and not more than 24 hours, after it experiences a disruption to a critical operation outside tolerance levels.

Paragraph 43 requires an APRA-regulated entity to maintain a systematic testing program for its business continuity plan, including the need to test the effectiveness of the entity's business continuity plan and the entity's ability to meet tolerance levels under a range of scenarios.

Paragraph 44 requires the systematic testing program to be tailored to the material risks of the regulated entity and include a range of severe but plausible scenarios, including disruptions to services provided by material service providers as well as scenarios with contingency arrangements. This paragraph allows APRA to require inclusion of an APRA-determined scenario as part of the entity's business continuity exercise.

Paragraph 45 requires the business continuity plan to be reviewed and updated at least annually to reflect specified changes within the APRA-regulated entity.

Paragraph 46 requires the internal audit function of an APRA-regulated entity to periodically review the business continuity plan, including providing assurance on certain matters to its Board.

*Management of service provider arrangements (paragraphs 47-61)*

Paragraph 47 requires an APRA-regulated entity to maintain a service provider management policy that includes details of how the entity will identify its material service providers, how it will manage material service provider arrangements and the material risks associated with the arrangements.

Paragraph 48 details matters that an APRA-regulated entity must include as part of its service provider management policy.

Paragraph 49 requires an APRA-regulated entity to identify its material service providers, maintain a register of its material service providers and to manage the risks arising from the use of such service providers. This paragraph also defines what constitutes a material service provider and material arrangement.

Paragraph 50 states that an APRA-regulated entity must classify providers who offer certain services as being material service providers unless the regulated entity is otherwise able to justify why a provider of a prescribed service should not be deemed a material service provider.

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

Paragraph 52 provides APRA discretion to require an APRA-regulated entity, or a class of APRA-regulated entities, to classify a particular service, or a type of service provider, as being material.

Paragraph 53 requires an APRA-regulated entity to do certain things before entering into an arrangement with a material service provider, or materially altering an existing arrangement. These things include undertaking appropriate due diligence and assessing the risks, both financial and non-financial, that could arise from reliance on a service provider.

Paragraph 54 requires an APRA-regulated entity to maintain a formal legally binding agreement with a material service provider. It also sets out matters that must be included as part of any such agreement.

Paragraph 55 sets out additional matters that the formally legally binding agreement under paragraph 54 must contain. These matters concern APRA's access to information and documentation, APRA's access to service providers to conduct on-site visits and that APRA is not impeded from fulfilling its duties as prudential regulator.



Paragraph 56 sets out matters that an APRA-regulated entity must undertake when it has an arrangement with a material service provider including identifying and managing risks that could affect provision of the service, other risks that could result from the arrangement, ensuring that the regulated entity's BCP is still able to be executed and ensuring the entity can exit the arrangement in need.

Paragraph 57 provides for APRA to require an APRA-regulated entity to review and to make changes to a service provider arrangement should APRA have heightened prudential concerns with respect to a particular arrangement.

Paragraph 58 requires an APRA-regulated entity to monitor and report on certain matters relating to the nature and usage of material service provider arrangements. The types of matters to be monitored and reported on include performance levels under the service provider agreement, the effectiveness of controls and compliance of both parties with the service provider agreement.

Paragraph 59 requires notification to APRA by an APRA-regulated entity when the entity enters into or materially changes an agreement for provision of a service that the regulated entity is reliant on in order to undertake a critical operation. A regulated entity must also notify APRA prior to entering into an offshoring agreement with a material service provider or when there is a significant change to an agreement.

Paragraph 60 requires the internal audit function of an APRA-regulated entity to review proposed outsourcing agreements with a material service provider for a critical operation of the APRA-regulated entity and to report either to the Board or Board Audit Committee of the regulated entity on compliance with the entity's service provider management policy for such arrangements.

### ***Exercise of discretion by APRA***

CPS 230 provides for APRA to exercise various discretions. Decisions made by APRA in exercising those discretions are not subject to merits review. This is because these decisions are preliminary decisions that may facilitate or lead to substantive decisions which are subject to merits review.

Under the Banking Act, Insurance Act, Life Insurance Act and PHIPS Act, a breach of a prudential standard is a breach of the enabling legislation, as each enabling Act provides that regulated entities must comply with the standard. Under the SIS Act, it is a condition on all RSE licences that the RSE licensee must comply with the RSE licensee law, which includes prudential standards. However, there are no penalties prescribed for breach of the prudential standards under any of these Acts. Instead, an entity's breach of the enabling legislation or RSE licence condition is grounds for APRA to make further, substantive decisions under the relevant enabling legislation in relation to the entity. Those decisions may include the decision:

- (a) to issue a direction to the regulated entity, including: a direction to comply with the whole or part of a prudential standard (section 11CA of the Banking Act, s.104 of the

Insurance Act, section 230B of the Life Insurance Act, section 131D of the SIS Act); and a direction to comply with all, or specified obligations, which includes prudential standards (section 96 of the PHIPS Act); or

- (b) to revoke: an authority to carry on banking business (section 9A of the Banking Act); a banking NOHC authorisation (section 11AB of the Banking Act); an authority to carry on insurance business (section 15 of the Insurance Act); an insurance NOHC authorisation (section 21 of the Insurance Act); registration of life insurance business (section 26 of the Life Insurance Act); a life NOHC authorisation (section 28C of the Life Insurance Act); or to revoke an authority to operate an APRA-regulated superannuation fund (section 29G of the SIS Act).

It is only at this stage that an entity is exposed to a penalty, loss of licence or imposition of a penalty if it breaches the direction (50 penalty units each day under section 11CG of the Banking Act, section 108 of the Insurance Act, and section 230F of the Life Insurance Act; 30 penalty units each day under section 104 of the PHIPS Act; and 100 penalty units each day under section 131DD of the SIS Act).<sup>1</sup> In nearly all cases,<sup>2</sup> the decisions are preceded by a full consultation with the regulated entity to raise any concerns they may have in relation to the decision.

The decisions of APRA to impose a direction are subject to merits review (section 11CA of the Banking Act, section 104 of the Insurance Act, section 236 of the Life Insurance Act, section 168 of the PHIPS Act and section 344 of the SIS Act), which is appropriately available at the point where an entity could be exposed to a penalty.

All decisions to revoke authorisations/registrations under the Banking Act, Insurance Act, Life Insurance Act and SIS Act are subject to merits review, unless specifically excluded by the enabling legislation.

Revocation of an authorisation to carry on banking business or a banking NOHC authorisation is subject to merits review unless either:

- (a) APRA has determined that access to natural justice and merits review is contrary to the national interest or contrary to the interests of depositors with the body corporate;
- or

---

<sup>1</sup> The exception is section 54B of the SIS Act, which provides that breach of a covenant under sections 52 or 52A is a civil penalty provision. The covenants include a requirement to comply with prudential standards in relation to specified topics (conflicts, capital requirements for operational risk, MySuper and choice products). CPS 230 is not a standard in relation to any of these topics.

<sup>2</sup> The Banking Act, Insurance Act and Life Insurance Act specifically provide that APRA does not need to consult where APRA is satisfied that doing so could result in a delay in revocation that would be contrary to the national interest or the interests of depositors with the body corporate (subsection 9A(4) of the Banking Act), contrary to the national interest (subsection 15(4) of the Insurance Act), or contrary to the public interest (subsection 26(5) of the Life Insurance Act), respectively.

(b) (in the case of ADIs only) the authority is an authority that is to cease to have effect on a day specified in the authority (subsection 9A(8) of the Banking Act).

Revocation of an authorisation to carry on insurance business or an insurance NOHC authorisation is subject to merits review (ss 15 and 21 of the Insurance Act).

Revocation of registration as a life insurance company or a life NOHC authorisation is subject to merits review (section 236 of the Life Insurance Act). The situation in relation to cancellation of registration under the PHIPS Act is different to the other enabling legislation.

### ***Adjust and exclude powers***

CPS 230 gives APRA the discretion to adjust or exclude a provision of the prudential standard (paragraph 11). The power to create such a discretion is provided for under subsections:

- 11AF(2) of the Banking Act;
- 32(3D) of the Insurance Act;
- 230A(4) of the Life Insurance Act;
- 92(4) of the PHIPS Act; and
- 34C(5) of the SIS Act.

APRA may exercise this power when it is satisfied that the adjustment or exclusion of a specific requirement for one or more specified regulated entities will better support APRA in meeting its objectives. For example, the adjustment or exclusion may be necessary to obtain a better prudential outcome than would be the case if the prudential requirement were applied unaltered to a particular regulated entity. A tailored approach would give APRA comfort that the prudential requirements apply appropriately to protect the interests of depositors, policyholders and fund members. APRA will also take into account other considerations, such as efficiency, competition, contestability, competitive neutrality and regulatory burden, including comparisons with an entity's peer group.

The exercise of APRA's powers is governed by a robust decision-making framework which is documented in APRA's internal policies. This framework supports APRA in fulfilling its mandate by limiting decision making to those senior APRA officers with the appropriate experience and skill to exercise prudent judgement. The framework also requires decision makers to seek advice from internal technical experts.

### ***Documents incorporated by reference***

Under section 14(1)(a) of the *Legislation Act 2003*, the standard incorporates by reference as in force from time to time:

- Acts of Parliament and associated delegated laws;
- Prudential Standards determined by APRA under:
  - subsection 11AF(1) of the Banking Act;
  - subsection 32(1) of the Insurance Act;
  - subsection 230A(1) of the Life Insurance Act; and
  - subsection 92(1) of the PHIPS Act.

Under section 14(1)(b) of the Legislation Act, where the standard incorporates by reference another Superannuation Prudential Standard determined by APRA under section 34C of the SIS Act, the Superannuation Prudential Standard referred to is the version that exists at the time the Instrument was determined.

All documents incorporated by reference in this standard are available on the Federal Register of Legislation at [www.legislation.gov.au](http://www.legislation.gov.au).

### **3. Consultation**

APRA undertook public consultation on the proposed CPS 230 from July to October 2022. This included consultation engagements with a variety of stakeholders including regulated entities and industry associations. APRA received 62 submissions in response to the consultation.

In July 2023, APRA released a detailed response to material issues raised submissions to the 2022 consultation, and the final CPS 230. APRA made a number of changes in finalising CPS 230 in response to issues and concerns raised during the consultation process. These included:

- deferring commencement from the original proposed date of 1 January 2024 to 1 July 2025;
- providing transitional relief in relation to existing contractual arrangements with service providers to allow sufficient time for entities to update such arrangements to ensure compliance with CPS 230;
- providing flexibility for a regulated entity to determine a prescribed critical operation should not be treated as a critical operation provided the entity is able to justify its decision; and
- providing flexibility for a regulated entity to determine that a prescribed material service provider is not a material service provider where the entity is able to justify its decision.

### **4. Regulation Impact Statement**

In developing CPS 230, APRA has followed a similar process to that required for a Regulation Impact Statement, which satisfies the requirements of the Office of Impact Analysis. The documents evidencing APRA's policy development process have been lodged as supporting material.

### **5. Statement of compatibility prepared in accordance with Part 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011***

A Statement of compatibility prepared in accordance with Part 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011* is provided at the Attachment to this Explanatory Statement.

## ATTACHMENT

### **Statement of Compatibility with Human Rights**

Prepared in accordance with Part 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011*.

### **Banking, Insurance, Life Insurance, Health Insurance and Superannuation (prudential standard) determination No. 2 of 2023**

The legislative instrument is compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011* (HRPS Act).

### **Overview of the Legislative Instrument**

The purpose of the instrument is to determine a new *Prudential Standard CPS 230 Operational Risk Management* (CPS 230).

CPS 230 sets out requirements to ensure that APRA-regulated entities are resilient to operational risks and disruptions and that risks arising from the use of service providers are managed appropriately.

CPS 230 seeks to ensure that APRA-regulated entities:

- identify and manage their operational risks;
- are able to continue to deliver critical operations to customers through severe disruptions; and
- have a comprehensive policy for managing risks from the use of service providers, and for the ongoing monitoring of such arrangements.

### **Human rights implications**

APRA has assessed the instrument and is of the view that it does not engage any of the applicable rights or freedoms recognised or declared in the international instruments listed in section 3 of the HRPS Act. Accordingly, in APRA's assessment, the instrument is compatible with human rights.

### **Conclusion**

The instrument is compatible with human rights as it does not raise any human rights issues.