**Banking, Insurance, Life Insurance, Health Insurance and Superannuation (prudential standard) determination No. 1 of 2018**

**Prudential Standard CPS 234 Information Security**

*Banking Act 1959*

*Insurance Act 1973*

*Life Insurance Act 1995*

*Private Health Insurance (Prudential Supervision) Act 2015 Superannuation Industry (Supervision) Act 1993*

I, Geoff Summerhayes, delegate of APRA:

1. under subsection 11AF(1) of the *Banking Act 1959*, DETERMINE *Prudential Standard CPS 234 Information Security* in the form set out in the Schedule, which applies to all ADIs and authorised banking NOHCs;

1. under subsection 32(1) of the *Insurance Act 1973* DETERMINE *Prudential Standard CPS 234 Information Security* in the form set out in the Schedule, which applies to all general insurers and authorised insurance NOHCs;

1. under subsection 230A(1) of the *Life Insurance Act 1995* DETERMINE *Prudential Standard CPS 234 Information Security* in the form set out in the Schedule, which applies to all life companies, including friendly societies, and registered life NOHCs;

1. under subsection 92(1) of the *Private Health Insurance (Prudential Supervision) Act 2015* DETERMINE *Prudential Standard CPS 234 Information Security* in the form set out in the Schedule, which applies to all private health insurers; and

1. under subsection 34C(1) of the *Superannuation Industry (Supervision) Act 1993* DETERMINE *Prudential Standard CPS 234 Information Security* in the form set out in the Schedule, which applies to all RSE licensees.

This instrument commences on 1 July 2019.

Dated: 30 November 2018

[Signed]

Geoff Summerhayes

Member

**Interpretation**

In this Determination:

***ADI*** has the meaning in section 5 of the *Banking Act 1959*. ***APRA*** means the Australian Prudential Regulation Authority.

***authorised banking NOHC*** has the meaning given to the expression authorised NOHC in section 5 of the *Banking Act* *1959*.

***authorised deposit-taking institution*** has the meaning given in section 5 of the *Banking Act 1959*.

***authorised insurance NOHC*** has the meaning given to the expression authorised NOHC in subsection 3(1) of the *Insurance Act* *1973*.

***friendly society*** has the meaning given in section 16C of the *Life Insurance Act 1995*.

***general insurer*** has the meaning given in section 11 of the *Insurance Act 1973*. ***life company*** has the meaning given in the Schedule to the *Life Insurance Act 1995*.

***private health insurer*** has the meaning given in section 4 of the *Private Health Insurance (Prudential Supervision) Act 2015*.

***registered life NOHC*** has the meaning given to the expression registered NOHC in the Schedule to the *Life Insurance Act 1995*.

***RSE licensee*** has the meaning given in section 10 of the *Superannuation Industry (Supervision) Act 1993*.

**Schedule**

*Prudential Standard CPS 234 Information Security* comprises the document commencing on the following page.

**Prudential Standard CPS 234**

**Information Security**

**Objectives and key requirements of this Prudential Standard**

This Prudential Standard aims to ensure that an APRA-regulated entity takes measures to be resilient against information security incidents (including cyberattacks) by maintaining an information security capability commensurate with information security vulnerabilities and threats.

A key objective is to minimise the likelihood and impact of information security incidents on the confidentiality, integrity or availability of information assets, including information assets managed by related parties or third parties.

The Board of an APRA-regulated entity is ultimately responsible for ensuring that the entity maintains its information security.

The key requirements of this Prudential Standard are that an APRA-regulated entity must:

* clearly define the information security-related roles and responsibilities of the Board, senior management, governing bodies and individuals;
* maintain an information security capability commensurate with the size and extent of threats to its information assets, and which enables the continued

sound operation of the entity;

* implement controls to protect its information assets commensurate with the criticality and sensitivity of those information assets, and undertake systematic testing and assurance regarding the effectiveness of those controls; and notify APRA of material information security incidents.

# Authority

1. This Prudential Standard is made under:

1. section 11AF of the *Banking Act 1959* (**Banking Act**);
2. section 32 of the *Insurance Act 1973* (Insurance Act);
3. section 230A of the *Life Insurance Act 1995* (Life Insurance Act);
4. section 92 of the *Private Health Insurance (Prudential Supervision) Act 2015* (PHIPS Act); and
5. section 34C of the *Superannuation Industry (Supervision) Act 1993* (SIS Act).

# Application

1. This Prudential Standard applies to all ‘APRA-regulated entities’ defined as:
   1. **authorised deposit-taking institutions** (**ADIs**), including **foreign ADIs**, and **non-operating holding companies** authorised under the Banking Act (authorised banking NOHCs);
   2. **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**;
   3. **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);
   4. **private health insurers** registered under the PHIPS Act; and
   5. RSE licensees under the SIS Act in respect of their business operations.[[1]](#footnote-1)
2. The obligations imposed by this Prudential Standard on, or in relation to, a

foreign ADI, a Category C insurer or an EFLIC apply only in relation to the Australian branch operations of that entity.

1. Where an APRA-regulated entity is the ‘Head of a group’,[[2]](#footnote-2) it must comply with a requirement of this Prudential Standard:
   1. in its capacity as an APRA-regulated entity;
   2. by ensuring that the requirement is applied appropriately throughout the group, including in relation to entities that are not APRA-regulated; and
   3. on a group basis.

In applying the requirements of this Prudential Standard on a group basis, references in paragraphs 13 to 36 to an ‘APRA-regulated entity’ are to be read as ‘Head of a group’ and references to ‘entity’ are to be read as ‘group’.

1. This Prudential Standard commences on 1 July 2019, subject to paragraph 6.
2. Where an APRA-regulated entity’s information assets are managed by a third party, the requirements in this Prudential Standard will apply in relation to those information assets from the earlier of the next renewal date of the contract with the third party or 1 July 2020.

# Interpretation

1. Terms that are defined in *Prudential Standard APS 001 Definitions* (APS 001), *Prudential Standard GPS 001 Definitions* (GPS 001), *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.

1. 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.
2. Where this Prudential Standard provides for APRA to exercise a power or discretion, the power or discretion is to be exercised in writing.
3. For the purposes of this Prudential Standard:

‘group’ means a Level 2 group or a **Level 3 group**, as relevant; ‘Head of a group’ means a Level 2 Head or **Level 3 Head**, as relevant;

‘Level 2 group’ means the entities that comprise:

* 1. **Level 2** as defined in APS 001; or
  2. a Level 2 insurance group as defined in GPS 001;

‘Level 2 Head’ means:

* 1. where an ADI that is a member of a Level 2 group is not a subsidiary of an authorised banking NOHC or another ADI, that ADI;
  2. where an ADI that is a member of a Level 2 group is a subsidiary of an authorised banking NOHC, that authorised banking NOHC; or
  3. the parent entity of a Level 2 insurance group as defined in GPS 001.

# Adjustments and exclusions

11. APRA may adjust or exclude a specific prudential requirement in this Prudential Standard in relation to an APRA-regulated entity.[[3]](#footnote-3)

# Definitions

12. The following definitions are used in this Prudential Standard:

1. *availability* refers to accessibility and usability when required;
2. *confidentiality* refers to access being restricted only to those authorised;
3. *criticality* refers to the potential impact of a loss of availability;
4. *information asset* means information and information technology, including software, hardware and data (both soft and hard copy);
5. *information security*means thepreservation of an information asset’s confidentiality, integrity and availability;
6. *information security capability* means the totality of resources, skills and controls which provide the ability and capacity to maintain information security;
7. *information security control* means a prevention, detection or response measure to reduce the likelihood or impact of an information security incident;
8. *information security incident* means an actual or potential compromise of information security;
9. *information security policy framework* means the totality of policies, standards, guidelines and procedures pertaining to information security;
10. *information security threat* (threat) is a circumstance or event that has the potential to exploit an information security vulnerability;
11. *information security vulnerability* (vulnerability) is a weakness in an information asset or information security control that could be exploited to compromise information security;
12. *integrity* refers to completeness, accuracy and freedom from unauthorised change or usage; and
13. *sensitivity* means the potential impact of a loss of confidentiality or integrity.

# Roles and responsibilities

1. The Board[[4]](#footnote-4) of an APRA-regulated entity (Board) is ultimately responsible for the information security of the entity. The Board must **ensure** that the entity maintains information security in a manner commensurate with the size and extent of threats to its information assets, and which enables the continued sound operation of the entity.[[5]](#footnote-5)
2. An APRA-regulated entity must clearly define the information security-related roles and responsibilities of the Board, senior management, governing bodies and individuals with responsibility for decision-making, approval, oversight, operations and other information security functions.[[6]](#footnote-6)

# Information security capability

1. An APRA-regulated entity must maintain an information security capability commensurate with the size and extent of threats to its information assets, and which enables the continued sound operation of the entity.
2. Where information assets are managed by a related party or third party, the APRA-regulated entity must assess the information security capability of that party, commensurate with the potential consequences of an information security incident affecting those assets.[[7]](#footnote-7)
3. An APRA-regulated entity must actively maintain its information security capability with respect to changes in vulnerabilities and threats, including those resulting from changes to information assets or its business environment.

# Policy framework

1. An APRA-regulated entity must maintain an information security policy framework commensurate with its exposures to vulnerabilities and threats.
2. An APRA-regulated entity’s information security policy framework must provide direction on the responsibilities of all parties who have an obligation to maintain information security.[[8]](#footnote-8)

# Information asset identification and classification

20. An APRA-regulated entity must classify its information assets, including those managed by related parties and third parties, by criticality and sensitivity. This classification must reflect the degree to which an information security incident affecting an information asset has the potential to affect, financially or nonfinancially, the entity or the interests of depositors, policyholders, beneficiaries or other customers.

# Implementation of controls

1. An APRA-regulated entity must have information security controls to protect its information assets, including those managed by related parties and third parties, that are implemented in a timely manner and that are commensurate with:
   1. vulnerabilities and threats to the information assets;
   2. the criticality and sensitivity of the information assets;
   3. the stage at which the information assets are within their life-cycle;[[9]](#footnote-9) and (d) the potential consequences of an information security incident.
2. Where an APRA-regulated entity’s information assets are managed by a related party or third party, the APRA-regulated entity must evaluate the design of that party’s information security controls that protects the information assets of the APRA-regulated entity.[[10]](#footnote-10)

# Incident management

1. An APRA-regulated entity must have robust mechanisms in place to detect and respond to information security incidents in a timely manner.
2. An APRA-regulated entity must maintain plans to respond to information security incidents that the entity considers could plausibly occur (information security response plans).
3. An APRA-regulated entity’s information security response plans must include the mechanisms in place for:
   1. managing all relevant stages of an incident, from detection to postincident review; and
   2. escalation and reporting of information security incidents to the Board, other governing bodies and individuals responsible for information security incident management and oversight, as appropriate.
4. An APRA-regulated entity must annually review and test its information security response plans to ensure they remain effective and fit-for-purpose.

# Testing control effectiveness

1. An APRA-regulated entity must test the effectiveness of its information security controls through a systematic testing program. The nature and frequency of the systematic testing must be commensurate with:
   1. the rate at which the vulnerabilities and threats change;
   2. the criticality and sensitivity of the information asset;
   3. the consequences of an information security incident;
   4. the risks associated with exposure to environments where the APRAregulated entity is unable to enforce its information security policies;[[11]](#footnote-11) and
   5. the materiality and frequency of change to information assets.
2. Where an APRA-regulated entity’s information assets are managed by a related party or a third party, and the APRA-regulated entity is reliant on that party’s information security control testing, the APRA-regulated entity must assess whether the nature and frequency of testing of controls in respect of those information assets is commensurate with paragraphs 27(a) to 27(e) of this Prudential Standard.[[12]](#footnote-12)
3. An APRA-regulated entity must escalate and report to the Board or senior management any testing results that identify information security control deficiencies that cannot be remediated in a timely manner.
4. An APRA-regulated entity must ensure that testing is conducted by appropriately skilled and functionally independent specialists.
5. An APRA-regulated entity must review the sufficiency of the testing program at least annually or when there is a material change to information assets or the business environment.

# Internal audit

1. An APRA-regulated entity’s internal audit activities must include a review of the design and operating effectiveness of information security controls, including those maintained by related parties and third parties (information security control assurance).
2. An APRA-regulated entity must ensure that the information security control assurance is provided by personnel appropriately skilled in providing such assurance.
3. An APRA-regulated entity’s internal audit function must assess the information security control assurance provided by a related party or third party where:
   1. an information security incident affecting the information assets has the potential to materially affect, financially or non-financially, the entity or the interests of depositors, policyholders, beneficiaries or other customers; and
   2. internal audit intends to rely on the information security control assurance provided by the related party or third party.[[13]](#footnote-13)

# APRA notification

1. An APRA-regulated entity must notify APRA as soon as possible and, in any case, no later than 72 hours, after becoming aware of an information security incident that:
   1. materially affected, or had the potential to materially affect, financially or non-financially, the entity or the interests of depositors, policyholders, beneficiaries or other customers; or
   2. has been notified to other regulators, either in Australia or other

jurisdictions.[[14]](#footnote-14)

1. An APRA-regulated entity must notify APRA as soon as possible and, in any case, no later than 10 business days, after it becomes aware of a material information security control weakness which the entity expects it will not be able to remediate in a timely manner.

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

# Prudential Standard CPS 230 Operational Risk Management

*Banking Act 1959*

*Insurance Act 1973*

*Life Insurance Act 1995*

*Private Health Insurance (Prudential Supervision) Act 2015 Superannuation Industry (Supervision) Act 1993*

I, John Lonsdale, a delegate of APRA:

1. under subsections 11AF(3) of the Banking Act, 32(4) of the Insurance Act, and 230A(5) of the Life Insurance Act, REVOKE *Banking, Insurance and Life Insurance (prudential standard) determination No. 6 of 2016* including *Prudential Standard CPS 231 Outsourcing* made under that determination;
2. under subsections 11AF(3) of the Banking Act, 32(4) of the Insurance Act, and 230A(5) of the Life Insurance Act, REVOKE *Banking, Insurance and Life Insurance (prudential standard) determination No. 7 of 2016* including *Prudential Standard CPS 232 Business Continuity Management* made under that determination;
3. under subsection 92(5) of the PHIPS Act, REVOKE *Health Insurance (prudential standard) determination No. 4 of 2015*, including *Prudential Standard HPS 231 Outsourcing* made under that determination;
4. under subsection 34C(6) of the SIS Act, REVOKE *Superannuation (prudential standard) determination No. 3 of 2012* including, *Prudential Standard SPS 231 Outsourcing* made under that determination, and *Superannuation (prudential standard) determination No. 4 of 2012* including *Prudential Standard SPS 232 Business Continuity Management* made under that determination;
5. under subsection 11AF(1) of the Banking Act,DETERMINEthe prudential standard which applies to all ADIs and authorised banking NOHCs;
6. under subsection 32(1) of the Insurance Act, DETERMINEthe prudential standard which applies to all general insurers and authorised insurance NOHCs and subsidiaries of general insurers and authorised insurance NOHCs;

1. under subsection 230A(1) of the Life InsuranceAct,DETERMINEthe prudential standard which applies to all life companies, including friendly societies, and registered NOHCs;
2. under subsection 92(1) of the PHIPS Act, DETERMINEthe prudential standard which applies to all private health insurers; and
3. under subsection 34C(1) of the SIS Act,DETERMINEthe prudential standard which applies to all RSE licensees.

This instrument commences on 1 July 2025.

Date: 11 September 2023

John Lonsdale

Chair

APRA

**Interpretation**

In this Determination:

***ADI*** has the meaning given in section 5 of the Banking Act. ***APRA*** means the Australian Prudential Regulation Authority.

***authorised banking NOHC*** has the meaning given to the expression *authorised NOHC* in section 5 of the Banking Act.

***authorised insurance NOHC*** has the meaning given to the expression *authorised NOHC* in subsection 3(1) of the Insurance Act.

***friendly society*** has the meaning given in section 16C of the Life Insurance Act.

***general insurer*** has the meaning given in section 11 of the Insurance Act.

***life company*** has the meaning given in the Schedule to the Life Insurance Act. ***private health insurer*** has the meaning given in section 4 of the PHIPS Act*.*

***registered NOHC*** has the meaning given in the Schedule to the Life Insurance Act.

***RSE licensee*** has the meaning given in subsection 10(1) of the SIS Act. ***the Banking Act*** means the *Banking Act 1959.* ***the Insurance Act*** means the *Insurance Act 1973*. ***the Life Insurance Act*** means the *Life Insurance Act 1995*.

***the PHIPS Act*** means the *Private Health Insurance (Prudential Supervision) Act 2015*.

***the prudential standard*** means *Prudential Standard CPS 230 Operational Risk Management in the form set out in the Schedule*.

***the SIS Act*** means the *Superannuation Industry (Supervision) Act 1993*.

**Schedule**

*Prudential Standard CPS 230 Operational Risk Management* comprises the document commencing on the following page.

**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:

1. section 11AF of the *Banking Act 1959* (Banking Act);
2. section 32 of the *Insurance Act 1973* (Insurance Act);
3. section 230A of the *Life Insurance Act 1995* (Life Insurance Act);
4. section 92 of the *Private Health Insurance (Prudential Supervision) Act 2015* (PHIPS Act); and
5. section 34C of the *Superannuation Industry (Supervision) Act 1993* (SIS Act).

# Application and commencement

1. This Prudential Standard applies to all APRA-regulated entities defined as:
   1. **authorised deposit-taking institutions** (**ADIs**), including **foreign ADIs**, and **non-operating holding companies** authorised under the Banking Act (authorised banking NOHCs);
   2. **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**;
   3. **life companies**, including **friendly societies**, **eligible foreign life insurance companies** (EFLICs) and **registered** **NOHCs**;
   4. **private health insurers** registered under the PHIPS Act; and
   5. registrable superannuation entity licensees (**RSE licensees)** under the SIS Act in respect of their business operations.[[15]](#footnote-15)
2. 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.

1. Where an APRA-regulated entity is the Head of a group,[[16]](#footnote-16) it must comply with a requirement of this Prudential Standard:
   1. in its capacity as an APRA-regulated entity;
   2. by ensuring that the requirement is applied appropriately throughout the group,[[17]](#footnote-17) including in relation to entities that are not APRA-regulated; and
   3. on a group basis.
2. 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’.
3. This Prudential Standard commences on 1 July 2025.
4. Where an APRA-regulated entity has pre-existing contractual arrangements in place with a service provider, the requirements in this Prudential Standard will apply in relation to those arrangements from the earlier of the next renewal date of the contract with the service provider or 1 July 2026.

# Interpretation

1. 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.
2. 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.
3. 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

11. APRA may adjust or exclude a specific prudential requirement in this Prudential Standard in relation to an APRA-regulated entity.[[18]](#footnote-18)

# Key principles

1. An APRA-regulated entity must:
   1. effectively manage its operational risks, and set and maintain appropriate standards for conduct and compliance;
   2. maintain its critical operations within tolerance levels through severe disruptions; and
   3. manage the risks associated with the use of service providers.
2. 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.
3. 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.
4. 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

1. 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:
   1. governance arrangements for the oversight of operational risk;
   2. an assessment of its operational risk profile, with a defined risk appetite supported by indicators, limits and tolerance levels;
   3. internal controls that are designed and operating effectively for the management of operational risks;
   4. appropriate monitoring, analysis and reporting of operational risks and escalation processes for operational incidents and events;
   5. 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
   6. processes for the management of service provider arrangements.
2. 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.[[19]](#footnote-19) The reviews must cover those aspects of operational risk management set out in paragraph 16.

1. 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 APRAregulated entity’s recovery and exit planning.[[20]](#footnote-20)
2. Where APRA considers that an APRA-regulated entity’s operational risk management has material weaknesses, APRA may:
   1. require an independent review of the entity’s operational risk management;
   2. require the entity to develop a remediation program;
   3. require the entity to hold additional capital, as relevant;[[21]](#footnote-21)
   4. impose conditions on the entity’s licence; and
   5. take other actions required in the supervision of this Prudential Standard.

# Roles and responsibilities

1. 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.[[22]](#footnote-22)
2. The Board must ensure that the APRA-regulated entity sets clear roles and responsibilities for **senior managers**[[23]](#footnote-23) for operational risk management, including business continuity and the management of service provider arrangements.
3. The Board must:
   1. 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 APRAregulated entity’s operational risk profile and ensure senior management takes action as required to address any areas of concern;
   2. approve the BCP and tolerance levels for disruptions to critical operations, review the results of testing and oversee the execution of any findings; and
   3. approve the service provider management policy, and review risk and performance reporting on material service providers.
4. 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.

# Operational risk management

1. 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-toend process for all business operations.
2. 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)*.*

## Operational risk profile and assessment

1. 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.[[24]](#footnote-24) This must include an assessment of the impact of new products, services, geographies and technologies on its operational risk profile.
2. An APRA-regulated entity must maintain a comprehensive assessment of its operational risk profile. As part of this, an APRA-regulated entity must:
   1. 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;
   2. 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
   3. 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.
3. An APRA-regulated entity must conduct a comprehensive risk assessment before providing a material service to another party, to ensure that the APRAregulated 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.Operational risk controls
4. 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.
5. 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.
6. 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

1. 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.
2. 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.[[25]](#footnote-25)

# Business continuity

34. An APRA-regulated entity must:

1. define, identify and maintain a register of its critical operations;
2. take reasonable steps to minimise the likelihood and impact of disruptions to its critical operations;
3. 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;[[26]](#footnote-26) (d) activate its BCP if needed in the event of a disruption; and

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

## Critical operations and tolerance levels

1. 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.
2. An APRA-regulated entity must, at a minimum, classify the following business operations as critical operations, unless it can justify otherwise:
   1. for an ADI: payments, deposit-taking and management, custody,

settlements and clearing;

* 1. for an insurer (general, life, private health): claims processing;
  2. for an RSE licensee: investment management and fund administration; and
  3. for all APRA-regulated entities: customer enquiries and the systems and infrastructure needed to support critical operations.

1. APRA may require an APRA-regulated entity, or a class of APRA-regulated entities, to classify a business operation as a critical operation.
2. For each critical operation, an APRA-regulated entity must establish tolerance levels for:
   1. the maximum period of time the entity would tolerate a disruption to the operation;
   2. the maximum extent of data loss the entity would accept as a result of a disruption; and
   3. minimum service levels the entity would maintain while operating under alternative arrangements during a disruption.
3. 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

1. An APRA-regulated entity’s BCP must include:
   1. the register of critical operations and associated tolerance levels;
   2. triggers to identify a disruption and prompt activation of the plan, and arrangements to direct resources in the event of activation;
   3. actions it would take to maintain its critical operations within tolerance levels through disruptions;
   4. 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
   5. a communications strategy to support execution of the plan.
2. An APRA-regulated entity must maintain the capabilities required to execute the BCP, including access to people, resources and technology.[[27]](#footnote-27) An APRAregulated entity must monitor compliance with its tolerance levels and report any failure to meet tolerance levels, together with a remediation plan, to the Board.
3. 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 taken, the likely impact on the entity’s business operations and the timeframe for returning to normal operations.

## Testing and review

1. 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.

1. The testing program must be tailored to the material risks of the APRAregulated 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.
2. 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.
3. 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

1. 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.
2. The policy must include:
   1. the entity’s approach to entering into, monitoring, substituting and exiting agreements with material service providers;
   2. the entity’s approach to managing the risks associated with material service providers; and
   3. 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.[[28]](#footnote-28)

## Material service providers

1. 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.[[29]](#footnote-29) Material arrangements are those on which the entity relies to undertake a critical operation or that expose it to material operational risk.
2. An APRA-regulated entity must, at a minimum, classify a provider of the following services as a material service provider, unless it can justify otherwise:
   1. for an ADI: credit assessment, funding and liquidity management and mortgage brokerage;
   2. for an insurer (general, life, private health): underwriting, claims management, insurance brokerage and reinsurance;
   3. for an RSE licensee: fund administration, custodial services, investment management and arrangements with promoters and financial planners; and
   4. for all APRA-regulated entities: risk management, core technology services and internal audit.
3. An APRA-regulated entity must submit its register of material service providers to APRA on an annual basis.
4. 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

1. Before entering into or materially modifying a material arrangement, an APRAregulated entity must:
   1. 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
   2. 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 on in providing the service.
2. For all material arrangements, an APRA-regulated entity must maintain a formal legally binding agreement (formal agreement). The formal agreement must, at a minimum:
   1. specify the services covered by the agreement and associated service

levels;

* 1. 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;
  2. include provisions to ensure the ability of the entity to meet its legal and compliance obligations;
  3. 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;
  4. require the liability for any failure on the part of any sub-contractor to be the responsibility of the service provider;
  5. include a *force majeure* provision indicating those parts of the contract that would continue in the case of a *force majeure* event; and
  6. 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).

1. The formal agreement must also include provisions that:
   1. allow APRA access to documentation, data and any other information

related to the provision of the service;

* 1. allow APRA the right to conduct an on-site visit to the service provider; and
  2. ensure the service provider agrees not to impede APRA in fulfilling its duties as prudential regulator.

1. For each material arrangement an APRA-regulated entity must:
   1. identify and manage risks that could affect the ability of the service provider to provide the service on an ongoing basis;
   2. identify and manage risks to the APRA-regulated entity that could result from the arrangement, such as step-in risk or contagion risk;
   3. ensure it can execute its BCP if needed; and
   4. ensure it can conduct an orderly exit from the arrangement if needed.
2. 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

1. 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:
   1. performance under the service agreement with reference to agreed service levels;
   2. the effectiveness of controls to manage the risks associated with the use of the service provider; and
   3. compliance of both parties with the service provider agreement.
2. An APRA-regulated entity must notify APRA:
   1. 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
   2. prior to entering into any material offshoring arrangement,[[30]](#footnote-30) 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.
3. An APRA-regulated entity’s internal audit function must review any proposed material arrangement involving the 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.

1. 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. [↑](#footnote-ref-1)
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. [↑](#footnote-ref-2)
3. 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. [↑](#footnote-ref-3)
4. 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. [↑](#footnote-ref-4)
5. A reference to the Board in the case of a foreign ADI, is a reference to the **senior officer outside Australia.**  [↑](#footnote-ref-5)
6. For the purposes of this Prudential Standard, governing bodies and individuals includes committees, working groups and forums. [↑](#footnote-ref-6)
7. For the avoidance of doubt, paragraph 16 of this Prudential Standard applies to all information assets managed by related parties and third parties, not only those captured under agreements with service providers of outsourced material business activities under *Prudential Standard CPS 231 Outsourcing* or *Prudential Standard SPS 231 Outsourcing*. [↑](#footnote-ref-7)
8. For the purpose of paragraph 19 of this Prudential Standard, parties includes governing bodies and individuals with responsibilities referred to in paragraph 14, as well as all other staff, contractors, consultants, related parties, third parties and customers. [↑](#footnote-ref-8)
9. The use of the term ‘life-cycle’ in this context refers to the process from planning and design through to decommissioning and disposal of an information asset. [↑](#footnote-ref-9)
10. For the avoidance of doubt, paragraph 22 of this Prudential Standard applies to all information assets managed by related parties and third parties, not only those captured under agreements with service providers of outsourced material business activities under *Prudential Standard CPS 231 Outsourcing* or *Prudential Standard SPS 231 Outsourcing*.

    [↑](#footnote-ref-10)
11. Also referred to as an ‘untrusted’ environment. [↑](#footnote-ref-11)
12. For the avoidance of doubt, paragraph 28 of this Prudential Standard applies to all information assets managed by related parties and third parties, not only those captured under agreements with service providers of outsourced material business activities under *Prudential Standard CPS 231 Outsourcing* or *Prudential Standard SPS 231 Outsourcing*.

    [↑](#footnote-ref-12)
13. For the avoidance of doubt, paragraph 34 of this Prudential Standard applies to all information assets managed by related parties and third parties, not only those captured under agreements with service providers of outsourced material business activities under *Prudential Standard CPS 231 Outsourcing* or *Prudential Standard SPS 231 Outsourcing*. [↑](#footnote-ref-13)
14. For the avoidance of doubt, paragraph 35 of this Prudential Standard applies to notifications of information security incidents not already captured as notifications under *Prudential Standard CPS 231 Outsourcing,* *Prudential Standard SPS 231 Outsourcing, Prudential Standard CPS 232 Business Continuity Management* or *Prudential Standard SPS 232 Business Continuity Management*. Other regulators include domestic government agencies and international regulators. [↑](#footnote-ref-14)
15. 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. [↑](#footnote-ref-15)
16. 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. [↑](#footnote-ref-16)
17. 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. [↑](#footnote-ref-17)
18. 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. [↑](#footnote-ref-18)
19. Refer to CPS 220 and SPS 220 for the requirement to undertake a review of the risk management framework. [↑](#footnote-ref-19)
20. Refer to *Prudential Standard CPS 190 Recovery and Exit Planning*. [↑](#footnote-ref-20)
21. 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*. [↑](#footnote-ref-21)
22. 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. [↑](#footnote-ref-22)
23. 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*. [↑](#footnote-ref-23)
24. 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. [↑](#footnote-ref-24)
25. 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. [↑](#footnote-ref-25)
26. An entity may have a number of BCPs. A BCP may include separate crisis management plans and disaster recovery plans. [↑](#footnote-ref-26)
27. 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. [↑](#footnote-ref-27)
28. A fourth party is a party that a service provider relies on in delivering services to an APRAregulated entity. [↑](#footnote-ref-28)
29. 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. [↑](#footnote-ref-29)
30. [↑](#footnote-ref-30)