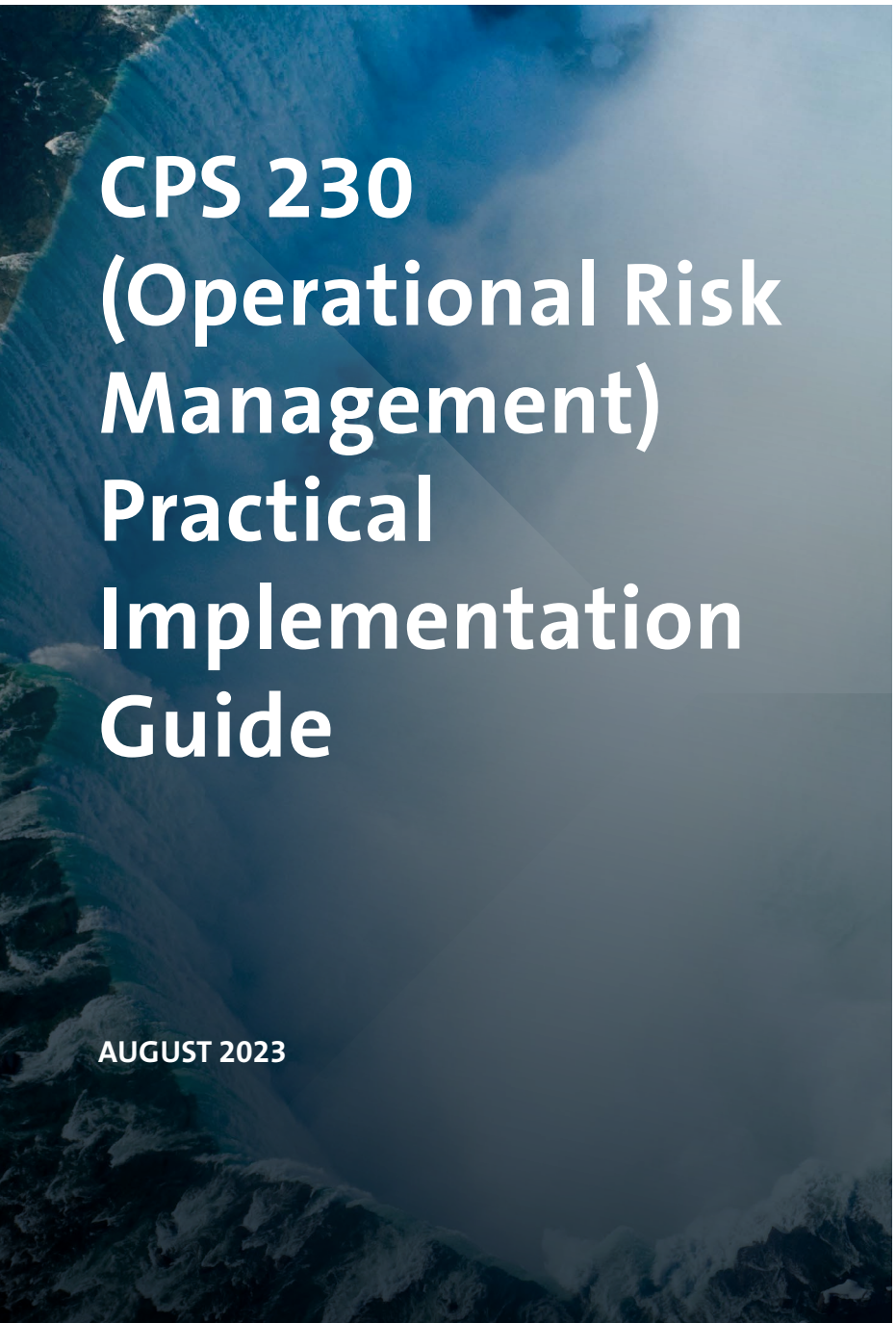
Allens

In alliance with Linklaters



CPS 230 (Operational Risk Management) Practical Implementation Guide

AUGUST 2023

Table of contents

Contents

1. Overview

IMPLEMENTATION

CPS 231, SPS 231 and HPS 231 Outsourcing

CPS 232 and SPS 232 Business Continuity Management

Replaced by

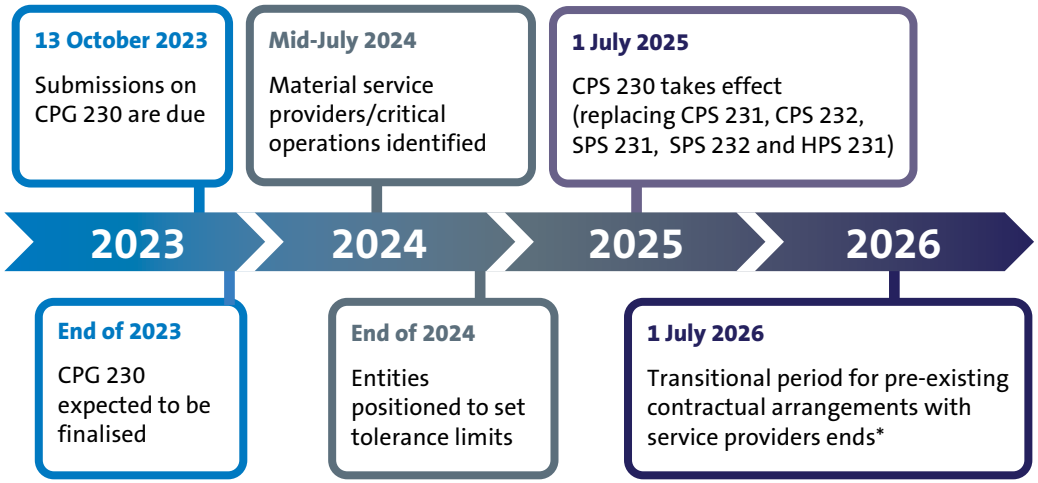
CPS 230 Operational Risk Management

CPS 220 and SPS 220 Risk Management

CPS 234 Information Security

APS 222 Associations with Related Entities

NEXT STEPS



** Where an APRA-regulated entity has pre-existing contractual arrangements in place with a service provider, CPS 230 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.*

WHO WILL BE AFFECTED?

All APRA-regulated entities will need to comply with the requirements set out in CPS 230[1]

- Authorised deposit-taking institutions (ADIs)
- General insurers
- Life insurers
- Private health insurers*
- RSE licensees (ie superannuation funds)
- Authorised or registered non-operating holding companies

Also applies to non-regulated entities within a group

Where an APRA-regulated entity is the head of a group, it must comply with the requirements of CPS 230 by ensuring the requirements are applied appropriately throughout the group, including in relation to entities which are not regulated by APRA.[2]

If your organisation provides services (directly or indirectly) to APRA-regulated entities, you may not be directly regulated by CPS 230, but you may still be affected

Your organisation may be contractually bound to comply with certain CPS 230 obligations under its agreements with APRA-regulated entities (or an upstream service provider to those entities) if you provide services which relate to a critical operation of the APRA-regulated entity or otherwise expose the entity to material operational risks.

** Private health insurers will now be required to comply with the same standards as other APRA-regulated entities. Previously, private health insurers were subject to less stringent standards under HPS 231 (which will be superseded by CPS 230)[3] and were not subject to the business continuity obligations imposed on financial institutions and RSE licensees under CPS 232 and SPS 232 respectively.*

2. Key takeaways

CPS 230 will require significant changes to governance, compliance, contractual and incident response arrangements for all APRA-regulated entities, which will need to:

1 Enhance operational risk processes, controls and framework

in order to meet the outcomes-based requirements of CPS 230, in line with the new focus on ensuring capability to continue to operate through disruption (rather than just recovery from disruption).

2 Enhance the governance arrangements for oversight of operational risk

as between the board, senior management and risk functions and ensure end-to-end responsibility for operational risk is embedded throughout the business.

3 Enhance business continuity plans

including identifying critical operations through the CPS 230 lens (including those functions which APRA has prescribed as critical), setting appropriate tolerance levels for each function and more extensive testing obligations.

4 Undertake a holistic assessment to identify material service providers and material arrangements

ie, those service providers and arrangements relied on for a critical operation or that expose the entity to a material operational risk, which are more expansive concepts than the existing 'material business activity' regime.

5 Develop a board-approved policy for managing risks of material service providers from end to end

which also looks deeper into the supply chain to subcontractors or 'fourth party' suppliers which are further downstream from the service provider directly appointed by the APRA-regulated entity.

6 Amend contracts for material arrangements

to meet the requirements of CPS 230.

7 Enhance reporting processes

to comply with APRA reporting timeframes, and prepare for increased APRA oversight and intervention in relation to operational risk.

Where an APRA-regulated entity is the head of a group, these obligations will need to flow appropriately throughout the group (including entities that are not regulated by APRA).

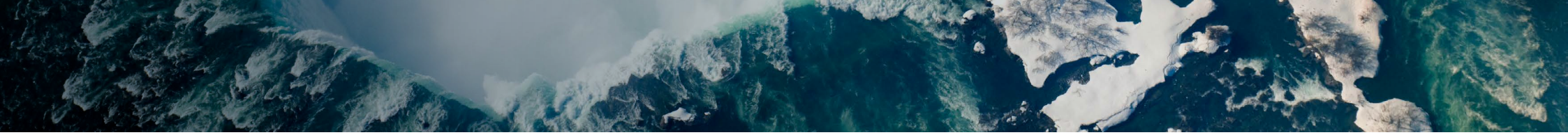
3. Roadmap to compliance

Of the requirements in CPS 230, some are entirely new, some are identical to existing requirements, some are similar to but more prescriptive or impose a slightly higher standard than existing requirements.

This roadmap outlines the steps regulated organisations should take to validate whether their existing processes and controls meet the new and more prescriptive requirements and uplifted standards set out in CPS 230. Further guidance is contained in draft CPG 230 and this roadmap should be considered in light of that guidance once finalised.

Governance

- [ ] Review and, if necessary, update your *operational* risk profile to ensure it is *comprehensively* assessed, including having regard to critical operations and interdependencies.[4]
- [ ] Ensure there are processes in place to reassess operational risk on an ongoing basis, including in light of business and strategic decisions (including in respect of new products, services, geographies and technologies),[5] any identified control gaps, weaknesses and failures,[6] and any operational risk incidents and near misses.[7]
- [ ] Ensure there is a framework in place to promptly identify and remediate *material weaknesses* in operational risk management, that sets out clear mechanisms for escalating issues, assigning responsibility and accountability, and conducting assurance, and which enables you to address the root causes of these weaknesses in a timely manner.[8]
- [ ] Uplift content requirements and triggers for *reporting* to the board, including to ensure that senior management reports on the expected impacts on critical operations of decisions which could affect the resilience of those operations.[9]
- [ ] Uplift board *approval* processes, including to ensure board approval of tolerance levels for disruption.[10] The board will also need to approve updates to the service provider management policy and business continuity plan (***BCP***) that are made in order to comply with CPS 230.[11]
- [ ] Update obligations libraries to reflect compliance with CPS 230, as well as related disclosure or issues registers and incident notification processes.
- [ ] Consider whether updates to internal roles and responsibilities are required, in order to embed operational risk management considerations.
- [ ] Update triggers and process for reporting to APRA, including to ensure notification following a disruption to a critical operation outside tolerance within 24 hours.[12]

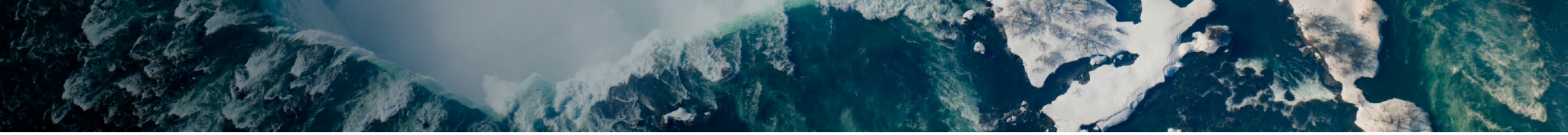


Business continuity management

> ***Operational resilience*** *is the outcome of prudent operational risk management: the ability to effectively manage and control operational risks and maintain critical operations through disruptions.*[13]

> ***Critical operations***[14] *are processes undertaken by a 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,*[15] *including (unless the entity can justify otherwise):*
>
> - *for an ADI: payments, deposit-taking and management, custody, settlements and clearing;*
> - *for an insurer (general, life, private health): claims processing;*
> - *for an RSE licensee: investment management and fund administration; and*
> - *for all APRA-regulated entities: customer enquiries and the systems and infrastructure needed to support critical operations.*[16]

- ☐ Maintain and monitor the age and health of information assets to meet business requirements and support critical operations and risk management.
- ☐ Identify critical operations and ensure that you can demonstrate that you have taken reasonable steps to minimise the likelihood and impact of disruptions to critical operations.[17]
- ☐ Set tolerance levels for each critical operation (including for maximum period of disruption, maximum extent of acceptable data loss and minimum service levels for alternative arrangements),[18] monitor compliance with those tolerance levels, and report any failure to meet them to the board.[19] APRA expects that entities will set and regularly reassess tolerance levels as they learn lessons from actual disruptions, testing, and evolution in industry practices.[20]
- ☐ Create a register of critical operations and the tolerance levels for each critical operation.[21]
- ☐ 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.[22]
- ☐ Update the BCP to include: (a) triggers to identify disruptions and promptly activate the BCP; (b) actions to be taken to maintain critical operations within tolerance levels through disruptions; (c) arrangements to direct resources following BCP activation; (d) assessments of execution risks, required resources, preparatory measures and key internal and external dependencies; and (e) a revised communications strategy which supports the revised BCP.[23] Work will also need to be undertaken to ensure the revised BCP interacts appropriately with cyber response plans and playbooks.
- ☐ Update internal processes and triggers for reviewing the BCP to ensure it is updated annually or where there are material changes to business operations (as is currently required), but also where there are changes in the 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.[24]
- ☐ Ensure you have the capabilities (including access to people, resources and technology)[25] required to execute the BCP, maintain disrupted critical operations within approved tolerance levels,[26] and promptly return disrupted operations to normal levels after disruptions.[27]
- ☐ Update business continuity testing controls and process. The testing requirements will be more prescriptive. Organisations will need a systematic testing program that includes an annual business continuity exercise[28] which tests the overall effectiveness of an entity's BCP and the entity's ability to maintain essential business operations within tolerance levels in a range of severe but plausible scenarios.[29] Those scenarios should include disruptions to services provided by material service providers and scenarios where contingency arrangements are required.[30]



Service provider management

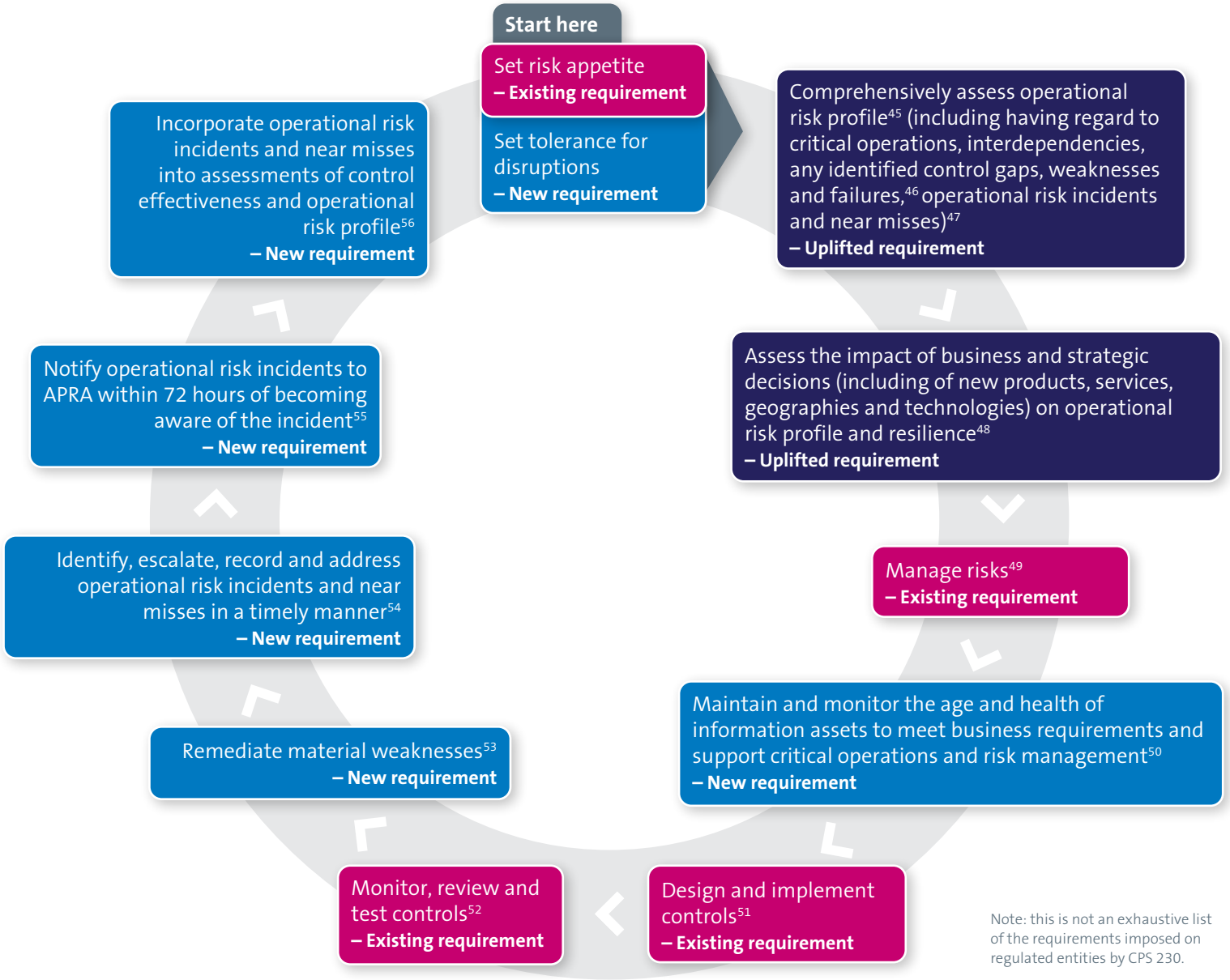
- [ ] Update your service provider management policy to apply not only to arrangements relied upon to undertake a critical operation (as is currently required), but *also* to arrangements that expose the organisation to *material operational risk*.[31] The policy should also be expanded to cover the approach to managing risks associated with any fourth parties relied upon by material service providers to deliver a critical operation to the APRA-regulated entity.[32]
- [ ] Identify and maintain a register of material service providers[33] and submit this register to APRA on an annual basis.[34] This is intended to facilitate APRA's monitoring of service provider concentration risk across the industry.
- [ ] Update procurement processes and processes for engaging with material service providers (including group entities) to ensure that:
  - [ ] before entering into, or materially modifying a material arrangement, you: (a) undertake appropriate due diligence; and (b) assess the financial and non-financial risks of relying on the service provider, including risks associated with geographic location or concentration of the supplier or parties the supplier relies on in providing the service;
  - [ ] you maintain a formal legal binding agreement (and where the entity is the head of a group, ensure all group entities also maintain)[35] in respect of all material arrangements, which includes the updated list of contractual terms set out in CPS 230;[36] and
  - [ ] approvals processes are updated to ensure that you do not rely on a service provider unless you can continue to meet prudential obligations and effectively manage the associated risks.[37]
- [ ] Update monitoring and internal reporting requirements to ensure more comprehensive and granular monitoring and reporting to senior management on material arrangements, including on performance under specific service agreements (by reference to agreed service levels), the effectiveness of controls to manage risks associated with the service provider, and compliance of both parties with the relevant agreement.[38]
- [ ] If you are a private health insurer, update APRA notification timeframes[39] and update audit capabilities in respect of material arrangements.[40]
- [ ] Update customer engagement processes to ensure it conducts a comprehensive risk assessment before providing a material service to another party to ensure that party can meet prudential obligations after entering into that arrangement.[41]

> ***Material service providers*** *are those on which the entity relies to undertake a critical operation or that expose it to material operational risk.*[42]

> ***Material arrangements*** *are those on which the entity relies to undertake a critical operation or that expose it to material operational risk.*[43]

4. Managing operational risks throughout their lifecycle

"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. This includes legal risk, regulatory risk, compliance risk, conduct risk, technology risk, data risk and change management risk.[44]"



Note: this is not an exhaustive list of the requirements imposed on regulated entities by CPS 230.

5. What will the board need to do?

The board of an APRA-regulated entity is ultimately accountable for the oversight of its operational risk management. [57]

THE BOARD NEEDS TO:

OVERSEE AND ENSURE

- Operational risk management[58]
  – existing requirement
- Clear roles and responsibilities for senior managers for operational risk management, including business continuity and the management of service provider arrangements[59]
  – existing requirement
- Senior management takes action to address any areas of concern[60]
  – existing requirement
- Effectiveness of key controls[61] and the implementation of any findings relating to the testing of key controls and the BCP[62]
  – existing requirement

APPROVE

- Tolerance levels for disruptions to critical operations, including as to the maximum period of disruption, the maximum extent of data loss and the minimum service levels to be maintained under alternative arrangements[63]
  – new requirement
- BCP[64]
  – new requirement
- Service provider management policy and any material changes to the policy[65]
  – new requirement

REVIEW

- Results of the testing of the BCP[66]
  – uplifted requirement
- Risk and performance reporting on material service providers[67]
  – uplifted requirement

Senior management needs to also ensure that the board gets the information it needs to:

- Understand financial and non-financial risks to the business.
- Monitor the entity's operational risk profile.[68]
- Understand the expected impacts on the entity's critical operations when the board is making decisions that could affect the resilience of critical operations.[69]

6. Expanding the scope of regulated service provider arrangements

FOCUS

CPS/SPS/HPS 231

Materiality of the service being provided

Regulates outsourcing of *material business activities* – being activities that have the potential, if disrupted, to have a significant impact on the entity's business operations or its ability to manage risk effectively[70]

Designates internal audit function and the risk management function as material business activities

CPS 230

Materiality of the risk posed by the arrangement

Regulates *material service providers* – being those on which the entity relies on to undertake a critical operation or that expose it to material operational risk,[71] whether that risk is related or unrelated to the entity, and whether this is a result of an individual arrangement or multiple arrangements with the entity[72]

Specifies that this includes the following service providers, unless the regulated entity can justify otherwise:

- for an ADI – credit assessment, funding and liquidity management and mortgage brokerage
- for an insurer (general, life, private health) – underwriting, claims management, insurance brokerage, and reinsurance
- for an RSE licensee – fund administration, custodial services, investment management and arrangements with promoters and financial planners
- for all APRA-regulated entities – risk management, core technology services and internal audit
- APRA classifies to be material (this may apply to a regulated entity or class of regulated entities)[73]

DEPTH OF SUPPLY CHAIN

CPS/SPS/HPS 231

Focusses on third parties

CPS 230

Expands focus to include consideration of the entity's approach to managing the risks associated with any fourth parties on which material service providers rely to deliver a critical operation to the APRA-regulated entity[74]

7. What will you need to notify or report to APRA?

	Event / Requirement	Further details	Timeframe	New or uplifted requirement
Notification event	Certain operational risk incidents	An operational risk incident that an entity 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[75]	As soon as possible and not later than 72 hours after becoming aware	***New requirement***
	Activation of 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[76]	As soon as possible and not later than 24 hours after it has suffered a disruption to a critical operation outside tolerance	***New requirement*** (for private health insurers) ***Uplifted requirement*** (for other regulated entities)
	Agreement for critical operation	Entering into or materially changing an agreement for the provision of a service on which the entity relies to undertake a critical operation[77]	As soon as possible and not more than 20 business days after	***Uplifted requirement***
	Offshoring arrangements	Entering into any material offshoring arrangement, or when there is a significant change proposed to the arrangement, including where data or personnel relevant to the service being provided will be located offshore[78]	Prior to entering into the arrangement or when there is a significant change proposed to the arrangement	***Uplifted requirement***
Reporting requirement	Requirement to submit register	Entity is required to submit their register of material service providers to APRA on an annual basis[79]	Annual	***New requirement***

8. APRA's powers

APRA can require a regulated entity to:

- Where it considers a regulated entity's operational risk management has material weaknesses, conduct an independent review of the entity's operational risk management, develop a remediation program, hold additional capital,[80] and take other actions required in the supervision of this standard.[81] APRA may also impose conditions on the entity's licence.

- Review and strengthen internal controls or processes where APRA considers there to be heightened prudential risks in circumstances where the entity is providing a material service to another party.[82]

- Classify a business operation as a critical operation (for the purposes of business continuity management).[83]

- Review and change its tolerance levels for a critical operation.[84]

- Adopt set tolerance levels where APRA identifies a heightened risk or material weakness.[85]

- Include an APRA-determined scenario in a business continuity exercise.[86]

- Classify a service provider, type of service provider, or service provider arrangement as material.[87]

- Review and make changes to a service provider arrangement where it identifies heightened prudential concerns.[88]

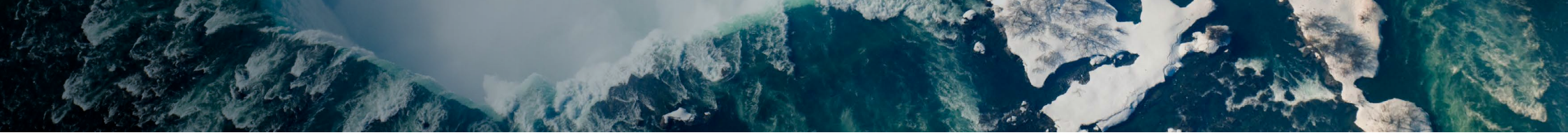
9. Key contacts

Valeska Bloch
Partner, Head of Cyber
T +61 2 9230 4030
Valeska.Bloch@allens.com.au

Stephanie Malon
Partner
T +61 408 676 523
Stephanie.Malon@allens.com.au

Geoff Sanders
Partner
T +61 410 096 472
Geoff.Sanders@allens.com.au

David Rountree
Partner
T +61 7 3334 3368
David.Rountree@allens.com.au



ENDNOTES

1 Prudential Standard CPS 230 – Operational Risk Management, para 2.
2 CPS 230, para 4.
3 Draft CPG 230, p.4.
4 CPS 230, para 27.
5 CPS 230, paras 26–7.
6 CPS 230, para 31.
7 CPS 230, para 32.
8 CPS 230, para 31.
9 CPS 230, para 23.
10 CPS 230, para 22(b).
11 CPS 230, paras 22(b) and 22(c).
12 CPS 230, para 42.
13 Draft CPG 230, para 1.
14 CPS 230, para35. Critical operations should be distinguished from the concept of 'critical functions' under CPS 900 (Resolution Planning), which refer to functions provided by an APRA-regulated entity that are important to financial system stability or the availability of essential function services to a particular industry or community (eg a very large deposit book).
The two concepts are distinguished by their focus and application:
- critical functions operate at the financial system-level and apply on a case-by-case basis, as determined by APRA; and
- critical operations operate at the entity-level and are defined and maintained by an entity within its BCP.

15 CPS 230, para 35.
16 CPS 230, para 36.
17 CPS 230, para 34(b).
18 CPS 230, para 38.
19 CPS 230, para 41.
20 Draft CPG 230, para 62.
21 CPS 230, para 40(a).
22 CPS 230, para 27(b).
23 CPS 230, para 40.
24 CPS 230, para 45.
25 CPS 230, para 41.
26 CPS 230, paras 12(b) and 14.
27 CPS 230, paras 14 and 34(e).
28 CPS 230, para 43.
29 CPS 230, para 16(e) and 43.
30 CPS 230, para 44.
31 CPS 230, para 47. The requirements for an 'outsourcing policy' under each of CPS 231 (which applies to financial institutions, general insurers and life insurers), SPS 231 (which applies to RSE licensees) and HPS 231 (which applies to health insurers) are relatively distinct, as the requirements under each are tailored to the type of APRA-regulated entities that are subject to those standards. CPS 230 proposes to align the requirements for all of these entities to develop a more general service provider management policy. As part of developing a new service provider management policy, regulated entities will need to make sure that their policies include registers of material service providers, approaches to changes of such providers, and approaches to risks associated with such providers (and any fourth parties they rely on).
32 CPS 230, para 48(c).
33 CPS 230, para 49.
34 CPS 230, para 51.
35 CPS 230, para 4 and 54.
36 CPS 230, para 54 and 55. CPS 230 includes a smaller number of more detailed requirements of contractual terms to be included in regulated arrangements, compared to those currently found in CPS 231 and SPS 231. However, these requirements represent a significant uplift when compared to the more limited terms under HPS 231 required by private health insurers to be included in an outsourcing arrangement that is covered by that standard. On request, we can provide a table containing a more granular comparison of CPS 230 and CPS 231.
37 CPS 230, para 15.
38 CPS 230, para 58.
39 CPS 230, para 59. CPS 230 contains similar notification requirements and timeframes to CPS 231 and SPS 231. However, the notification requirements from private health insurers will be slightly different. Previously under HPS 231, private health insurers were required to notify APRA within 28 days of entering or terminating an outsourcing agreement and provide APRA with a risk assessment and risk controls developed in relation to such agreement (see para 24), whereas under CPS 230, private health insurers will be required to notify APRA within 20 business days of entering into or materially changing an agreement in relation to a critical operation or an offshoring agreement (see para 59).
40 CPS 230, para 28 and 60. CPS 230 contains similar audit requirements to CPS 231 and SPS 231. However, private health insurers, which were previously not subject to any audit requirements under HPS 231, will need to significantly uplifted their audit capabilities.
41 CPS 230, para 28.
42 Section 49, CPS 230.
43 Section 49, CPS 230.
44 CPS 230, paragraphs 13 and 24.
45 CPS 230, para 27.
46 CPS 230, para 31.
47 CPS 230, para 32.
48 CPS 230, para 26–7.
49 CPS 230, para 24.
50 CPS 230, para 25.
51 CPS 230, para 29.
52 CPS 230, para 30.
53 CPS 230, para 31.
54 CPS 230, para 32.
55 CPS 230, para 33.
56 CPS 230, para 32.
57 CPS 230, para 20.
58 CPS 230, para 22(a).
59 CPS 230, para 21.
60 CPS 230, para 22(a).
61 CPS 230, para 22(a).
62 CPS 230, para 22(b).
63 CPS 230, paras 22(b) and 38.
64 CPS 230, para 22(b).
65 CPS 230, para 22(c); CPS 230, para 20.
66 CPS 230, para 22(b).
67 CPS 230, para 22(c).
68 CPS 230, para 27(a).
69 CPS 230, para 23.
70 The factors organisations currently need to have regard to under Prudential Standard CPS 231 – Outsourcing, para 14, include:
- the financial and operational impact and impact on reputation of a failure of the service provider to perform over a given period of time;
- the cost of the outsourcing arrangement as a share of total costs;
- the degree of difficulty, including the time taken, in finding an alternative service provider or bringing the business activity in-house;
- the ability of the APRA-regulated institution or member of the group to meet regulatory requirements if there are problems with the service provider;
- potential losses to the APRA-regulated institution's or group's customers and other affected parties in the event of a service provider failure; and
- affiliation or other relationship between the APRA-regulated institution or group and the service provider.

71 CPS 230, para 49.
72 CPS 230, footnote 15.
73 CPS 230, para 50.
74 CPS 230, para 48(c).
75 CPS 230, para 33.
76 CPS 230, para 42.
77 CPS 230, para 59(a).
78 CPS 230, para 59(b).
79 CPS 230, para 51.
80 For example, APRA may require an RSE licensee to meet an ORFR target amount determined by APRA under Prudential Standard SPS 114 (Operational Risk Financial Requirement) (see CPS 230, footnote 7).
81 CPS 230, para 19(e).
82 CPS 230, para 28.
83 CPS 230, para 37.
84 CPS 230, para 39.
85 CPS 230, para 39.
86 CPS 230, para 44.
87 CPS 230, para 52.
88 CPS 230, para 57.