Actuaries Institute.

CPS 230 Implementation

Presented by:

Alison Bliss, Mike Devine, Justine Cameron and Barry Leung

Important notice for all participants

This meeting is being conducted in accordance with Institute's Code of Conduct and attended by members in their professional capacity.

It is acknowledged that professional members in their employed capacity, may be active market participants in their respective industries who may compete with each other as defined by competition law.

Participants are, therefore, reminded that in accordance with their competition law compliance obligations they should not:

- discuss any matter that may be perceived as being cooperation by competitors in a market to influence that market;
- discuss any matters that could be regarded as fixing, maintaining or controlling prices, allocation of customers or territories, coordinating bids and/or restricting output or acquisitions in any circumstances;
- share commercially sensitive information relating to their employer; or
- share information for an anti-competitive purpose.

How does CPS230 impact your day-to-day work

- ❑ Directly implementing CPS230 at my workplace
- ❑ Consulting the implementation of CPS230
- ❑ Not implementing CPS230 project but it will impact to my day-to-day
- ❑ No direct impact, here to learn more about CPS230

Actuaries Institute.

Which industry do you work/ consultant in ?

- ❑ General Insurance
- ❑ Life Insurance
- ❑ Superannuation
- ❑ Banking
- ❑ Health
- ❑ Other

Actuaries Institute.

Actuaries Institute.

Mike Devine

APRA

Head of Operational Resilience - Transformation

Mike joined APRA in July 2021 as a Risk Specialist as part of the Operational Risk team. During this role Mike was focused on oversight of Regulated Entity Risk Transformation programs as well as supporting capability development in Operational Risk and related risk classes (i.e. Compliance Risk and Data Risk).

Mike has worked in Operational Risk Management in first and second lines of defence roles across both Banking and Insurance for brands including Commonwealth Bank, IAG, and Suncorp. During his time in industry Mike has been part of some of Australian Financial Services' largest risk transformation and remediation programs.

Prior to moving to Financial Services Mike worked as a Research Lead and Academic for the Queensland University of Technology Business School. Mike holds a Doctor of Philosophy (Risk Management) and Master of Business (Organisational Culture).

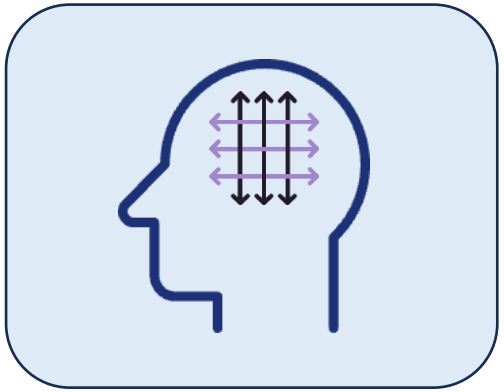
Insights Sharing

Key Milestones

- Release of CPG230 and supporting response paper.
- Greater transparency with inclusion of the CPS230 Supervisory Program and Compliance Checklist.
- APRA Preparedness Meeting Series with 35+ entities and Material Service Provider (MSP) roundtables.

Key Themes

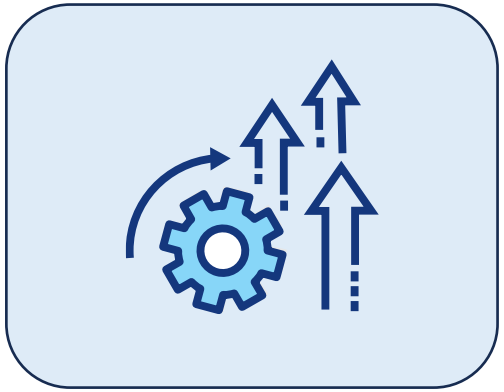
- Shifting mindsets to a Critical Operations view of operational risk is a key enabler for success.
- Pilot programs enable teams to ensure programs are right-sized for their size, business mix, and complexity.
- Accountability for Critical Operations and the role of Risk Management teams in oversight.
- Sustainability past completion of the ‘project’ is a key area of interest for stakeholders in industry.



Mindset Shift

Pilot Programs

Accountability



Sustainability

Actuaries Institute.

CPS 230 Supervision Programme

Year approach is SFI focused.

Year two extends prudential review programme into non-SFIs.

Material Service Provider (MSP) register submission commences from
1 October 2025.

	2025-26	2026-27	2027-28
SFIs	**Prudential review** with a small subset of entities.	**Prudential review** with another subset of entities.	BAU ongoing supervision.
Non-SFIs	**Prudential meeting** with reviews on exceptions basis only.	**Prudential review** with a small subset of entities.	**Prudential review** with another subset of entities.
All entities	• Notifications (event-based, reactive). • Submit Material Service Provider register. • Heightened supervision if entity is an MSP outlier or a material event occurs. • APRA to field queries, offer practice insights.		APRA may consult on a formal reporting standard.

Actuaries Institute.

Response to submissions - CPG 230 Operational Risk Management | APRA

CPS 230 Compliance Checklist

Requirement	Submission to APRA	Updated or New Requirement
Critical Operations (COs) are identified	Entities are not required to submit their list of critical operations. However, an APRA supervisor could request it.	**NEW** as concept of critical operations is introduced by CPS 230.
Tolerances are defined and approved by the Board for COs (time, data loss, and service level)	Entities are not required to submit tolerance lists. However, an APRA supervisor could request it, to understand how critical operations are monitored and to confirm Board approval as required by the Standard.	**UPDATE** as tolerances exist under CPS 232 for time and SLAs. CPS 230 applies a Critical Operations lens.
Material Service Providers (MSPs) are identified	Entities are required to submit a register of MSPs to APRA on an annual basis. APRA requests the first submission by 1 Oct 2025. This is the key data requirement of CPS 230 along with incident notifications and supplier/offshore notifications.	**NEW** but building on the requirements that have been in place under CPS 231, in monitoring and oversight of suppliers.
Notifications are operational for material events, tolerance breaches and MSP changes	Entities are required to have notifications to APRA in place per paragraphs 33 (material events), 49 (tolerance breach) and 59 (MSP arrangement/offshoring changes).	**UPDATE** as notification requirements do exist under CPS 231 and CPS 232 in the current architecture.
Board Governance & Oversight is in place and clear roles and responsibilities are set	Entities are not required to submit updated senior management accountabilities or target operating model documentation. This could be requested and discussed as part of a prudential review.	**UPDATE** to align with the critical operations requirements in CPS 230 but builds on CPS 220 positioning.
Risk Profiles & Reporting is established and supporting oversight accountabilities	Entities are not required to submit risk profiles or risk reporting as part of compliance with CPS 230. These could be requested and discussed as part of a prudential review.	**UPDATE** against critical operations and building on CPS 220, 231, 232 foundations.
Accountability for COs, MSPs, and monitoring is in place	Entities are not required to submit updated operational accountabilities or examples of BAU monitoring, reporting or controls for compliance with CPS 230. These could be requested as part of a prudential review.	**UPDATE** to accountabilities, to refer to new concepts introduced under CPS 230 building on CPS 220, 231, 232 foundations.
Contract Updates have an extension of 12 months per paragraph 7 of the standard*	Entities have an additional 12 months to ensure that pre-existing service provider arrangements comply with contract requirements under CPS 230.	**UPDATE** to pre-existing contracts to comply with CPS 230.
Business Continuity Management (BCM) shifts to a Critical Operations focus*	Entities are not required to submit their updated BCM strategy, policy, or plans. These could be requested and discussed as part of a prudential review.	**UPDATE** of existing BCM policy, plans, testing under CPS 232 to the CPS 230 Critical Operations focus.
Scenarios align with BCM uplift and focus on severe yet plausible scenarios for Critical Operations and Material Service Providers*	Entities are not required to submit their new scenarios or testing results as part of CPS 230 compliance. This could be requested and discussed as part of a prudential review.	**UPDATE** of existing scenario approach under CPS 232 to apply a CPS 230 critical operations lens.

*From 1 July 2026 for all entities *Components of BCM and Scenarios commence from 1 July 2026 for non-SFIs

Actuaries Institute.

[Response to submissions - CPG 230 Operational Risk Management | APRA]

Actuaries Institute.

Barry Leung

MIPS

Executive General Manager – Performance

Barry is a seasoned executive with over 20 years of experience in insurance and healthcare, including his current role as Executive General Manager, Performance at MIPS, a national medical indemnity organisation.

He has experience working in the healthcare and insurance sectors, holding senior roles across major health insurers including Medibank and Defence Health. Barry is passionate about better health for all. Prior to joining MIPS, he was an Impact Insurance Fellow with the International Labour Organisation, advising the National Health Insurance Authority in Ghana West Africa on the country's universal health cover scheme.

Our Approach to implementation

- Critical Operations Identification and mapping
  - Business Capability Framework
- Business Resilience
  - Business Impact analysis
  - Maximum tolerance setting
  - Testing
  - Documentation
- Material Service Provider
  - Material Service Provider (MSP) Policy - update
  - Identification of MSP (against critical operations or prescribed)
  - Risk and contract assessment
  - Negotiation with existing providers
- Operational Risk Management
  - Design and implement template for risk profile across enterprise and divisions
  - Control testing
  - Operational risk reporting
  - Risk assessment artefacts for new products or key changes

These three streams goes hand in hand in the overall standard implementation

Actuaries Institute.

Challenges

Business Resilience

- Process mapping and interdependencies
- Disruption scenario construct – what is a plausible disruptive event?
- Testing and reporting resourcing
- Keep processes underpinning critical operations up to date
- Education to enable setting and approval of tolerance levels

Material Service provider

- Inflight MSPs and contract negotiation
- What if the MPS does not agree to minimum requirement mandated in the standards?
- Fourth party – notification and assurance

Actuaries Institute.

Challenges

Operational Risk management

- Consistent “language” across Board and management
- Robust incident management system to enable identification of systematic risks and root cause analysis
- Incidents do not “drag on” and closed within committed timeframe
- Scenario testing and interaction with other artefacts (e.g. ICAAP and recovery plan)

Overall

- Interaction with other existing (e.g. CPS234) and upcoming standards (e.g. FAR)
- Number of regulatory changes to implement (noting proportionality and extensions)
- Board education and involvement
- Level of complexity vs maturity required
- Resourcing to adopt and maintain for a small entity

Actuaries Institute.

Opportunities

- Material service provider
  - Embed a culture of monitoring and improvement -> getting value for money from the service
  - Consider exit strategy as part of contract (re)negotiation
  - Clear ownership of relationship with service providers (and thus responsibilities associated with it)

- Scenario Testing
  - Holistic approach enterprise wide – operational impact and capital
  - Consequential impact of a scenario – think of second or third order impact
  - Financial and non-financial impact considered

- Operational risk management
  - Explicit end to end understanding and documentation of critical operations / processes
  - Enhanced Board & senior management engagement and education
  - Formalisation and strengthening of arrangements within the Group
  - Maturing linkages to Risk Appetite and Key Risk Indicators

Actuaries Institute.

Justine Cameron

AIA

General Manager, Legal

Justine is a senior adviser and compliance expert with over twenty years' experience and an expert focus on providing pragmatic advice in strategically important matters.

Justine was the General Counsel and regulatory legal expert at several different financial services organisations and is now a General Manager in the Enterprise Risk & Compliance team at AIA Australia, leading the change program to implement CPS 230 and the Financial Accountability Regime. She is passionate about simplification and partnering to resolve difficult problems and get the best out of people. As well as being a proven trusted C-suite advisor to Boards, Committees, senior executives and stakeholders she has been an independent director and chaired the Finance and Risk Management Committee for an ASIC-regulated public institution.

HEALTHIER, LONGER, BETTER LIVES

Actuaries Institute

CPS 230 Implementation

August 2024

AIA confidential and proprietary information. Not for distribution.

Project Resilience

Background: CPS 230 Operational Risk Management (CPS 230) will be effective on 1 July 2025 and the Financial Accountability Regime (FAR) will commence on 15 March 2025 for insurers.

These regulatory changes provide an opportunity to:

- integrate and build on our current initiatives and strengthen our operational risk resilience
- strengthen responsibility and accountability frameworks and improve governance culture

Program Resilience has been set up to address the requirements under CPS 230 and the FAR.

APRA CP230 requires us to

- Strengthen operational risk management
- Enhance business continuity management
- Enhance service provider management

FAR requires us to

- Have clearly defined accountabilities across all accountable persons in an entity

Enterprise Obligation

Provide greater visibility of risk performance practices and insights to senior management, Board and APRA

Intended Business Outcome

- identify, assess and manage operational risks, with effective internal controls, monitoring and remediation;
- be able to continue to deliver critical operations within approved 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.

CPS230 and FAR will shift the way we manage risk and will safeguard our sustainability

Spotlight on: Critical Operations, Business Continuity, Service Provider Management, Risk Management Governance, Executive Accountabilities

AIA confidential and proprietary information. Not for distribution.

[AIA - INTERNAL]

Implementation Milestones

CPS 230

- **Identify CPS 230 Critical Operations**
- **Prepare end-to-end Process Maps**
- **Clarify accountability for Critical Operations**
- **Link Critical Operations to the BCP**
- **Set tolerance levels for disruption**

AIA confidential and proprietary information. Not for distribution.

[AIA - INTERNAL]

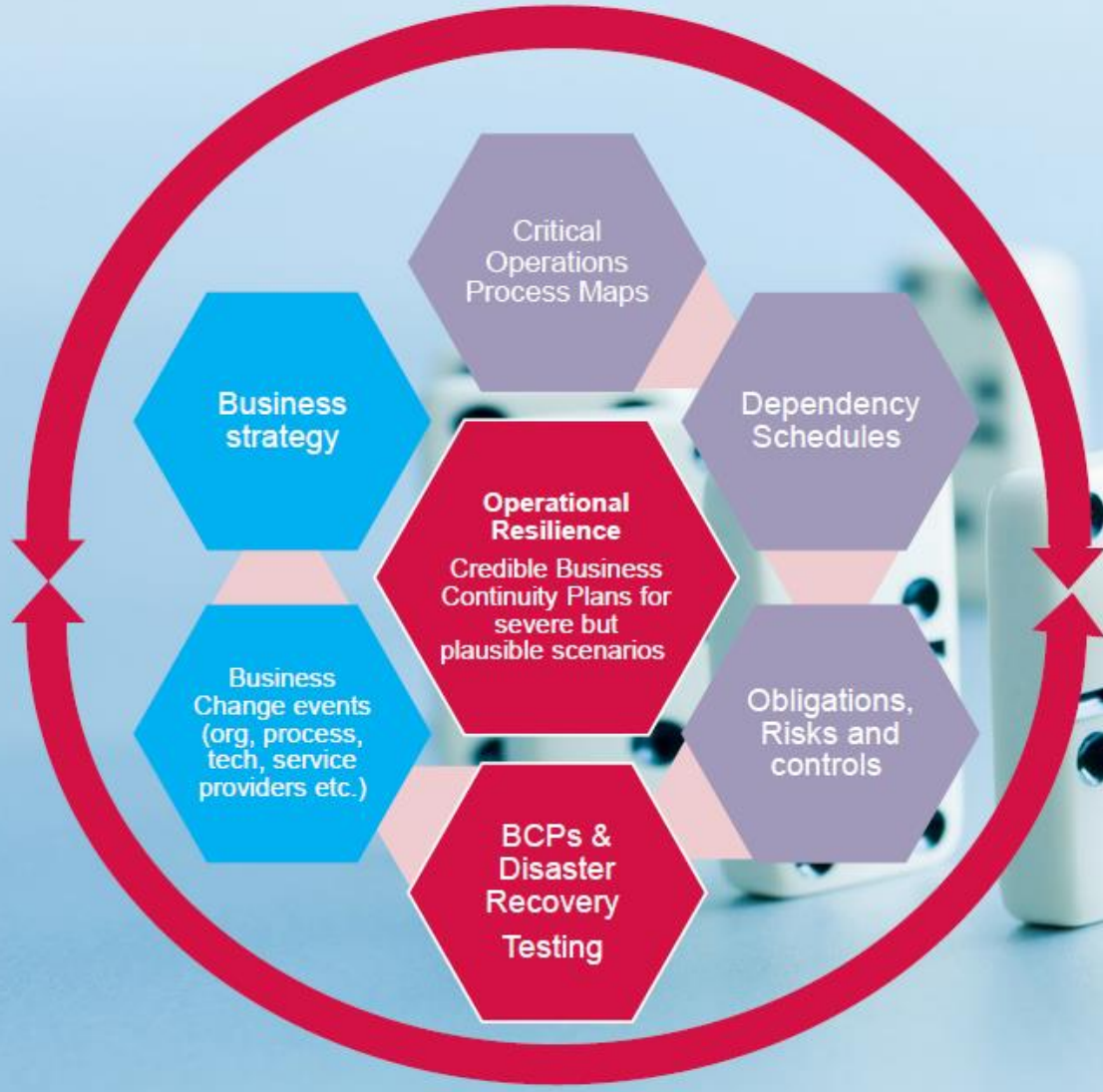
AIA Program Resilience Overview

Critical Operations	Business Continuity Management	Service Provider Management	Risk Management Framework & Governance
• Identify and map critical operations (Level 2) including related assets, dependencies, sub processes, risks, obligations and controls • Set tolerance levels across all critical processes	• Design and implement new Business Continuity Management framework and operating model (incl testing and monitoring process) aligned to CPS 230 requirements • Embed new tolerance levels for critical operations into Business Continuity Planning process • Scenario development and testing	• Identify 'material service providers' and set up a monitoring process • Uplift contractual arrangements with 'material service providers' • Implement changes required to current service provider management framework • Design and adopt comprehensive new policy for service provider management aligned to CPS 230 requirements	• Reflect CPS 230 changes into the AIA Risk Management Framework • Uplift Board oversight and reporting • Remediate material weaknesses in operational risk management as mandated by CPS 230

AIA confidential and proprietary information. Not for distribution.

[AIA - INTERNAL]

A bottom-up approach and understanding of our Critical Operations and all the dependencies that impact them is fundamental to minimizing disruptions and strengthening operational resilience.



Link 'CPS 230' Critical Operations to the Business Continuity Plans

3) Business Continuity Plans

Critical Operations (CPS 230)

Disruption impact - Material Adverse impact to Customer, Entity or Financial System

Essential Business Functions

Business RTO < 72 Hrs (AUS)

Disruption impact BIA of 3 Minor and 1 Moderate

Business Impact Analysis (BIA) – Impact Threshold Matrix

Description	Direct / Indirect Financial/ Operational Loss	Fines and Sanctions	Customer Outcome	Reputation
1 Minimal	Direct loss or increased cost of up to 0.5% of Local OPAT or up to USD4m	Non-systematic Breaches with no adverse impact or not reportable to regulator	Minor detriment to a small group of customers	Local media attention is quickly remedied with public awareness but not concern
2 Minor	Direct loss or increased cost of up to 1% of Local OPAT or between USD4m to USD8m	A few non-systemic Breaches or reportable Incidents with no follow up corrective required	Minor detriment to a large group of customers	Local reputational damage on local news or social media
3 Moderate	Direct loss or increased cost of up to 3% of Local OPAT or between USD8m to USD20m	Multiple related minor Breaches reportable to the local regulator with immediate correction to be implemented	Moderate detriment to a large group of customers	National short-term negative media coverage causing decreased support from shareholders or the community

2) Business Impacts Assessment

All Business Processes

1) Severe but Plausible Scenario generation

Facilities | Critical Staff | IT systems / applications | Service Providers | Internal dependent depts

Inputs

Sub Process

Disruption

Outputs

Legend: Critical Operation, Essential Business Function, Non-Essential

AIA confidential and proprietary information. Not for distribution.

[AIA - INTERNAL]

Outcome

How will Critical Operations process maps strengthen our operational risk management?

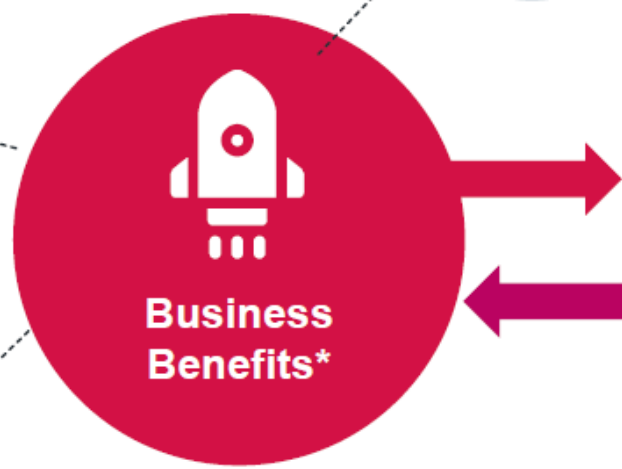
Benefit 1. Greater clarity about our Critical Operations

Simple, holistic, end to end view of our Critical Operations will make it easier to understand, control, test and minimize material risks that may impact our ability to serve our customers

A strong awareness and understanding of all the Critical Operations processes

Benefit 2. Increased alignment and new opportunities for Preventative Risk Management

Comply with APRA's definition when identifying AIA's Critical Operations, and embed this language uniformly into our risk management practices



Understanding the nuances and individual services each business unit has in place.

Benefit 3. Simplification through bottom-up alignment (critical ops business continuity risk profile)

Moving forward we will leverage the Critical Ops Maps as we introduce changes to identify and manage risk in a more targeted, timely and effective manner. This will include updating BCPs more regularly

How departments link with Claims or help support Claims Operations.

* *Details set out in appendix A*

AIA confidential and proprietary information. Not for distribution.

[AIA - INTERNAL]

Q&A Session

Actuaries Institute.

Actuaries Institute.

Thank you

Actuaries Institute
actuaries.asn.au