Australian Custodial Services Association

CPS 230 OPERATIONAL RISK

Guidance Note for Scenario Testing for ACSA Members and Clients

31 July 2025

TABLE OF CONTENTS

Introduction

Australian Prudential Regulation Authority ("APRA") released the final CPS 230 ("CPS 230") Operational Risk Management Prudential Standard ("Prudential Standard") in July 2023 and the accompanying Prudential Practice Guide ("PPG") in June 2024.

The Prudential Standard is effective from 1 July 2025 and introduces substantial changes to the way APRA-regulated entities are to oversee and manage arrangements with services providers, including custodians. Entities that are classified as "non-Significant Financial Institutions" have an additional 12 months to comply with certain requirements in CPS 230 relating to business continuity and scenario analysis. For pre-existing contracts with service providers, CPS 230 will apply from the earlier of the next contract renewal date or 1 July 2026.

APRA have indicated its expectations that APRA-regulated entities identify their critical operations and material service providers by mid-2024 and set their tolerance levels by end of 2024. APRA also included a "Day 1" checklist for entities to assist in their implementation of CPS 230. Refer to Figure 3. The checklist clarifies what information entities are not required to provide to APRA for Day 1 compliance (but which may be requested by APRA). For example, entities are not required to submit their list of critical operations or tolerance levels to APRA on Day 1 nor risk profiles or operational and senior accountabilities.

ACSA Guidance Note

The impact of CPS 230 on the members of the Australian Custodial Services Association ("ACSA"), as material service providers to many APRA-regulated clients ("ACSA member clients"), will be significant, increasing client expectations with respect to reporting, escalation, access, and data. Whilst not all ACSA members are regulated by APRA, custodians are captured under CPS 230 as a Material Service Provider.

ACSA established a CPS 230 Working Group to collaboratively review the implications of this Prudential Standard and develop a Critical Operations guidance note for ACSA's members and its clients to leverage. This guidance note also considered high level outcomes from engagements with other industry bodies as it relates to scenario testing with material service providers, however ACSA expects members and member clients to determine their own response.

This guidance note is general in nature and does not consider all nuances that may exist. It is the responsibility of each individual APRA regulated entity to perform their own independent assessment and, if necessary, secure their own independent advice on the regulations to ensure compliance with the regulations. As per the final APRA Prudential Standard, APRA-regulated entities approach to operational risk must be appropriate to its size, business mix and complexity.

About this guidance note

APRA requires APRA-regulated entities to have a systematic testing program for its Business Continuity Program that covers all critical operations and includes an annual business continuity exercise.

Severe but plausible scenarios should be used to the test the effectiveness of the entity's critical operation sand its ability to meet tolerance levels.

Severe but plausible scenarios would be defined as situations that would result in high impact and significant disruptions to critical operations, and while unlikely to occur, remain probable.

ACSA Guidance Note on Scenario Testing and Design compliments the previously issued Guidance Notes on Critical Operations, Impact Tolerance and Oversight arrangements.

When determining a framework for scenario testing and design, ACSA has prepared areas that should be contemplated when working with your material service provider.

Scope and approach

- Objectives of testing:
  - Evaluate the business response and recovery actions deployed for a specific operational disruption event to validate the ability of the Critical Operation to remain within its defined tolerance level during severe but plausible disruption scenarios.
  - This will include the evaluation of response and recovery actions, including:
    - The time, resources and oversight required to deliver each action.
    - The communication strategies used internally and externally.
  - Confirm their Critical Operations ability to remain within its Tolerance Level and/or identify conditions in which it would not be either possible or prudent to do so. This includes ensuring that: (i) the Maximum Allowable Outage (MAO) has been appropriately set and (ii) to confirm its applicability to processes that directly support the Critical Operation against a list of severe yet plausible scenarios.
  - Identification of vulnerabilities and/or potential areas for enhancement as a core element of the exercise outcome.
  - Confirmation of the communication strategy to clarify the scope and approach of who needs to be communicated with internally and externally (including clients, fund managers, regulators, custodians, depository/clearing)

- Severe but Plausible Scenario tests can include disruptions to:
  - technology
  - third parties
  - location
  - people
  - data, data centres, data storage, and
  - geopolitical events impacting Critical Operations (volatility, inability to buy/sell assets etc).

- Frequency:
  - Critical Operations should be tested at least once within a multi-year program (recommendation on a 3 year cycle)

- Approach to testing:
  - Minimum one scenario for each Critical Operation. Each scenario could either be unique to a specific Critical Operation or applicable to more than one Critical Operation.
  - The design of each scenario can be based on:
    - Residual risks, emerging risks and/or findings from actual operational disruption events, including external events and near misses.
    - one or more specific resources, processes or controls (or combinations thereof) from the analysis of the Process Maps of a Critical Operation
    - severity, plausibility and variation from previous scenario exercises.

- Participants:
  - Participants of a scenario test should be driven by the selected scenarios and Critical Operations, which would typically include (but not limited to):
    - staff within the organisation (i.e. Critical Operation(s) owner(s) and teams, business continuity management team or coordinator(s), technology team, facilities teams and/or other support teams where relevant)
    - Material service providers as documented on the “APRA MSP register” or as part of formal industry scenario testing.

- Scenario test options:
  - Paper based – involves review of existing documentation and interviews with impacted stakeholders to determine the scenario and impacts. Conclusions are drawn based on existing documentation.
  - Group walkthrough – integrated workshop based involving a wider group of stakeholders. Typically in a controlled environment with scenario inject input by facilitators.

- Live simulation – activities involving mobilisation of senior stakeholders, operations or technology teams to activate business continuity, crisis or disaster recovery plans to see real time responses.

Scenario testing

- A risk-based approach is used to define the minimum requirements for testing scenarios and recovery capabilities.

- The scope for each exercise should be documented, including associated dependencies to be tested, test participants, test objectives and success criteria. The scope of processes to be tested is outlined in each dependency (e.g. location, people, technology etc) category.

- Test activities, results and evidence are collected/documented, reviewed and retained. Any issues identified from testing and items for consideration and/or remediation should be captured and tracked through to timely remediation in accordance with the issue management framework employed by each entity.

- Reporting should be performed through to management and the Board on the outcomes of test results, any issues arising (including the impact to the resilience of Critical Operations) and timeframes for remediation.

Scenario test design dependency considerations

Location & People Dependency

- Critical Operations may be supported out of a single location or multiple locations. The process maps and metadata (if available) tagged against Critical Operations are useful tools in identifying concentration risk. If there are cohorts of staff in particular locations that would be impacted if there is a disruption event affecting a whole location (e.g. cyclones, power outage). Identifying and testing recovery capabilities and transfer of work from one location to another may reduce concentration risks and form part of the scenario test.

- Consider the impact to the loss of locations both onshore and offshore (where applicable).

- Key personnel supporting Critical Operations should be considered if they are unavailable.

- Material service providers will have different location and people dependency and strategies. All entities are encouraged to discuss with their MSP.

Technology Dependency

- Technology and data centres are critical components of the Critical Operation value chain. A severe disruption could lead to systems and infrastructure not being available for a prolonged period with potentially no alternative arrangements. The identification of technology in the process mapping supporting Critical Operations can identify areas of risk that may require a review of the criticality of that application.

- An entity may have specific scenario focusing on severe disruption of data centres and applications and/or factor in technology dependencies into other scenarios.

- When recovering from technology outages, consider system recovery order and whether the collective Recovery Time Objectives (RTOs) to recover systems would impact tolerances around maximum period of disruption.

Data Dependency

- Data recovery testing validates that a system's data can be restored from a severe disruption event. The extraction of critical business data from this secondary site (or other sources available) and recovery of lost data ensures minimal data loss and business continuity.

- Each system will have its own disaster recovery and back up strategy and timelines which will inform whether Recovery Point Objectives (RPOs) can be met.

- Consider whether data can be re-keyed into systems from other source systems. As part of this, the manual effort to complete this should be considered in the context of maximum allowable outages (MAO) and minimum service levels (MSL).

Third Party Dependency

- Disruption events for Third Parties are similar to that of ourselves as material service providers (i.e. temporary disruption of service provision) but may also include bankruptcy or insolvency (i.e. permanent cessation of service provision). Where relevant, all entities should understand the recovery capabilities of external Third Parties, and how your organisation's recovery capability will work with theirs in the event of a business disruption and the impact to your Critical Operations.

- The Third Party would have their own Business Continuity Plans and would be part of the ongoing management of material service providers in ensuring any risks or issues identified are escalated and remediation actions put in place accordingly. Organisations should have in place a framework and a set of requirements for reviewing and/or assuring testing performed by third parties. This should be part of ongoing governance and performance discussions with third parties.

- Third Party testing would be based on either the criticality of the process or the business criticality of the Third Party's application or service.

- Consider conducting third party dependency testing with critical third parties (noting this may need to be included in contractual uplifts).

- Temporary alternative arrangements for the loss of critical Third Parties (if available) should be factored into testing.

Risk reduction

Critical Operation - ability to operate within tolerances
Findings, or risks to the Critical Operations ability to remain within its Tolerance Limit, are identified throughout the implementation of the Operational Resilience Framework. In particular, identification is expected as a result of mapping, scenario testing or items for consideration from actual operational disruption events. Any breaches of tolerances through actual operation disruption events will need to be reported internally and to APRA.

Scenario Test Failures
Where a scenario test completely or partially fails for high criticality operations, the resolution of the finding should be documented and appropriately remediated in a timely manner. Reporting should be provided on scenario test failures to management and Boards.

Metrics, Monitoring and Reporting

Operating Reports
Entities could consider implementing regular reporting of key metrics to Governance Committees to demonstrate adoption of, and compliance with, program requirements.

Monitoring and Reporting
Formalising documentation and attestation on a periodic basis that recovery plans are functional, have been successfully tested, and are following program and applicable regulatory requirements.

Oversight Arrangements
Service provider may have differences in how their Scenario Testing and Design operates to manage the risks in how their businesses are structured.
Transparency and confidence in the framework and the implementation of those frameworks can be achieved through ongoing service reviews, annual due diligence and independent assurance programs where internal frameworks, controls and risk management can be verified are working effectively.

Example of a Scenario Test

Each entity should identify their own severe but plausible scenarios having regard their own unique business model set up and dependencies. There are some generic examples of the types of disruption that could occur to an APRA Regulated entity including but not limited to:

- Sub process platforms that are material to the generation and distribution of the NAV or Unit Pricing that are not available
- Fund accounting platform not available to generate the NAV or Unit Pricing
- Third party market data vendor not available that impacts Critical Operations
- Fund manager data not available due to disruption within their business or their Third Party that is required in delivering your Critical Operations.
- Natural disaster, pandemic, war, political unrest, or wide scale power outages impacting local team or key offshore service provider supporting Critical Operations
- Unavailability of primary data centre or key IT infrastructures or applications due to cyber event (i.e. hacking, DDOS attack, ransomware, etc)
- Severe internet latency issue or complete outage

Conclusion:

Under APRA's CPS230 requirements the **ACSA Guidance Note on Scenario Testing and Design** seeks to aid APRA-regulated entities and their material service providers to enhance their operational resilience through systematic and risk-based scenario testing.

By incorporating severe but plausible scenarios into their Business Continuity Programs, entities can evaluate the effectiveness of their Critical Operations with sufficient rigor and ensure they remain within defined tolerance levels during disruptive events.

About the Australian Custodial Services Association (ACSA)

The Australian Custodial Services Association (ACSA) is the peak industry body representing members of Australia's custodial and investment administration sector. Our mission is to promote efficiency and international best practice for members, our clients and the market. ACSA works with peer associations, governments, regulators and other market participants on a pre-competitive basis to encourage standards, process consistency, market reform and operating efficiency. Established in 1994, ACSA members currently hold assets in excess of $4.5 trillion in custody and under administration for Australian institutions (at 31 December 2024).

The key sectors supported by ACSA members include large superannuation funds and investment managers, as well as other domestic and international institutions. Custodians provide a range of institutional services to clients including traditional custody and safekeeping, investment administration, foreign exchange, securities lending, transfer agency, tax and financial reporting, investment analytics (risk, compliance and performance reporting), investment operations middle office outsourcing and ancillary banking services.

www.acsa.com.au

CPS 230 OPERATIONAL RISK