

CPS 230

OPERATIONAL RISK

Guidance Note:
CPS 230 Tolerance Levels

Effective Date
December 2024
Version 1.0

TABLE OF CONTENTS

| | |
|-----------------------------------------------------|-------|
| Introduction | 3 |
| ACSA Guidance Note..... | 3 |
| Tolerance Level Setting Guide..... | 4 |
| Risk and Impact Assessment..... | 4 |
| Establishing Tolerance Levels..... | 5 |
| Tolerance Setting Guidance..... | 6 |
| Steps and Consideration in Setting Tolerances..... | 7 |
| Commencement of CPS 230..... | 9 |
| Key Considerations for APRA Regulated Entities..... | 9 |
| Glossary of Terms..... | 10-11 |
| Important Note..... | 12 |



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.

This guidance note continues the work of The Australian Custodial Services Association (“ACSA”) and builds on the issuance of its [CPS 230 Guidance Note on Critical Operations issued in July 2024](#) and Tolerance Setting in December 2024

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 guidance note to assist ACSA’s members and its clients manage the oversight of their material service providers.

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.

Tolerance Level Setting Guide

ACSA's guide for tolerance level setting supports ACSA members and their client's operational resilience and compliance with CPS 230. It helps ACSA members and their clients consider how to approach establishing and setting of tolerance levels which align with APRA's regulatory standard and guideline.

This guide is an **ACSA approach** for setting tolerances levels that may impact ACSA members clients, financial markets and /or the custodian and considers:

- Disruptions could be **triggered** by people, facilities, service providers, technology (resources) or market related events
- **Accountability** and management of resiliency risk sits with the APRA regulated entity
- **ACSA members** responsibility is to review their service provider framework to ensure operational risks are appropriately monitored and managed in the event of a severe disruption
- Standard recovery time objectives may **not apply** in the event of a severe but plausible disruption where **business continuity plans and disaster recovery are both materially impacted**
- **Minimum Service Levels** are the resources required to be restored to deliver critical operations; Timelines to restore a critical operation can vary depending on the levels of automation within that process


Risk and Impact Assessment

Setting operational resilience tolerance levels involves establishing clear, measurable thresholds for acceptable levels of disruption in critical services, operations and applications. This process is crucial for identifying, assessing, and managing operational risks, ensuring that custodial services can continue to operate effectively amidst various challenges. This includes:

- **Comprehensive Risk Assessment:** Conduct thorough risk assessments to identify potential operational risks, including security breaches, equipment failures, cyber-attacks, and human errors.
- **Stakeholder Involvement:** Engage with all relevant stakeholders, including custodial service providers, regulatory bodies, and security agencies, to gather comprehensive insights into potential risks.
- **Data Analysis:** Utilise historical data and predictive analytics to understand the likelihood and impact of different risk scenarios.

Establishing Tolerance Levels

Establishing tolerance levels is intended to help the business understand the point at which direct/indirect material adverse impact occurs to customers, the broader financial system or economy. Once you have understood and documented the critical operation, the following tolerance levels need to be determined:






CPS 230, para 38 requires organisations to establish tolerance levels:

For each critical operation, an APRA-regulated entity must establish tolerance levels for:

- The maximum period of time the entity would tolerate a disruption to the operation.
- The maximum extent of data loss the entity would accept as a result of a disruption.
- Minimum service levels the entity would maintain while operating under alternative arrangements during a disruption.

Establishing tolerance levels is intended to help the business understand the point at which direct/indirect material adverse impact occurs to customers, the broader financial system or economy. Once you have understood and documented the critical operation, the following tolerance levels need to be determined:

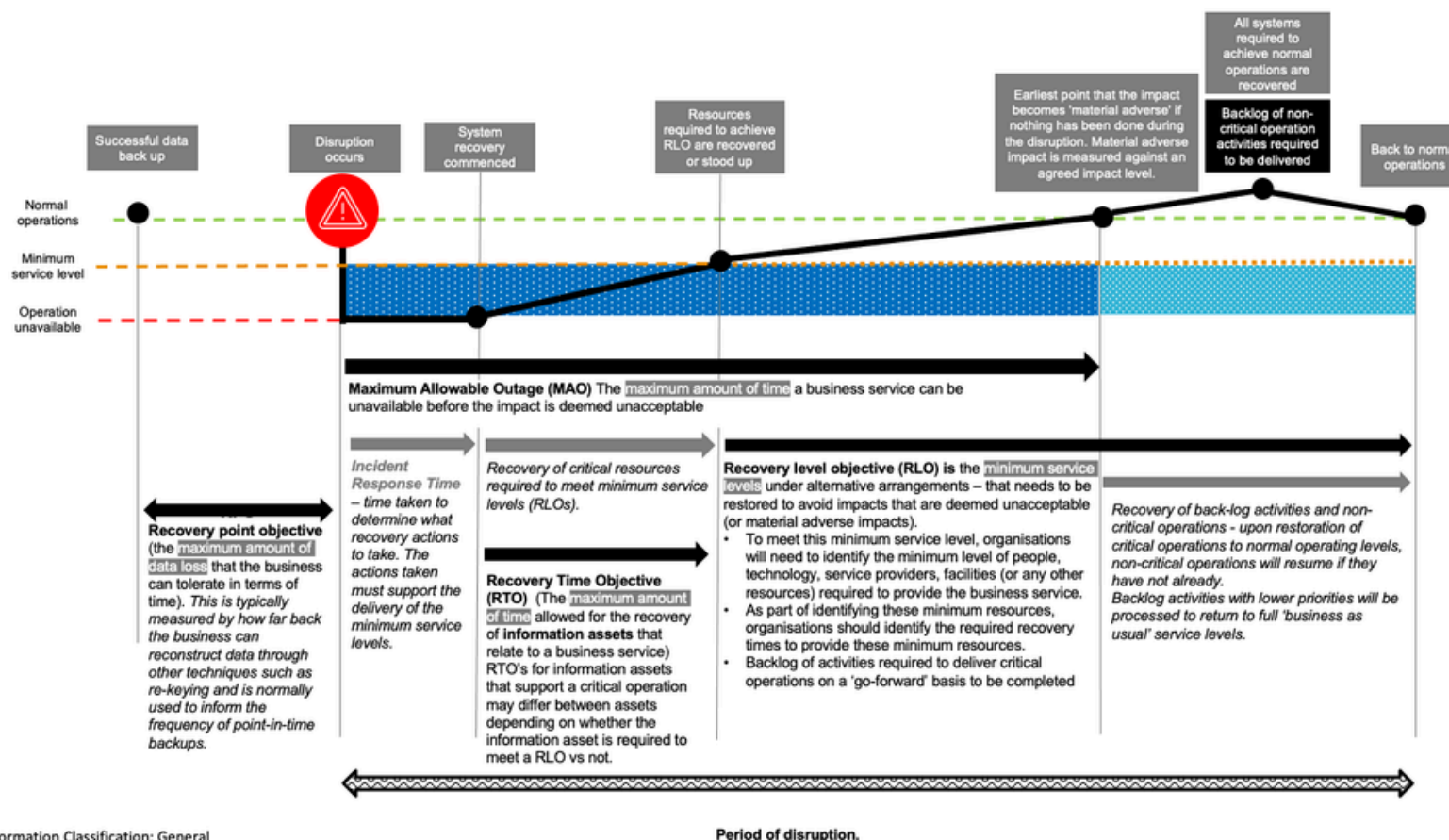
|  Maximum period of time |  Maximum data loss |  Minimum service levels |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> Maximum allowable outages (the maximum amount of time a business service can be unavailable before the impact is deemed unacceptable). <p>Note that maximum allowable outages (MAO) may already exist in the Business Impact Analysis (BIAs) which can have other terminologies such as 'maximum disruption time'</p> <ul style="list-style-type: none"> Recovery time objectives (the maximum amount of time allowed for the recovery of information assets that relate to a business service), which is typically less than the maximum allowable outage to allow time to initiate recovery activities. <p>It is common to have RTOs for the existing applications and systems. However, CPS 230 requires a desired RTO that is consolidated at the end-to-end process level that will be approved by the board.</p> | <ul style="list-style-type: none"> Recovery point objective (the maximum amount of data loss that the business can tolerate in terms of time). This is typically measured by how far back the business can reconstruct data through other techniques such as re-keying and is normally used to inform the frequency of point-in-time backups. In APRA's view, sound practice is to accept that there are scenarios where data can be lost (because of issues with data replication), meaning the maximum data loss should never be set at zero. <p>RPOs may not exist in the current BIAs and therefore, need to be established.</p> | <ul style="list-style-type: none"> Recovery level objective (the minimum level of service that needs to be restored to avoid impacts that are deemed unacceptable). An entity would normally establish a recovery level objective when resumption to business-as-usual operations would require a protracted period of time. An entity would normally determine the minimum level of people, information assets and other resources required to provide the business service. <p>These tolerances are relatively new to the industry and therefore need to be established.</p> |

ACSA members should:

- Discuss the **custodial services** that form part of its clients critical operations with their clients
- Provide clients with an overview of its approach to establishing tolerances having regard to the principles/requirements outline above
- Obtain an understanding of their clients tolerances having regard to the custodial service provided with a view to assessing potential vulnerabilities
- Continue to engage with clients as tolerances are refined over time
- While ACSA members may have similar critical operations the tolerances established for these critical operations may vary from custodian to custodian as a result of different operating models, nature and size of the business (including client base) and technology platforms.

Tolerance Setting Guidance



ACSA provides guidance on operational resilience tolerance setting to help ACSA members and their clients. Establishing resilience tolerances is vital for fostering trust among stakeholders and maintaining the integrity of financial markets during disruption, reinforcing ACSA's commitment to supporting a robust and secure custodial services industry.








Steps and Consideration in Setting Tolerances

After mapping the critical operation and the relevant resources needed, workshops are typically conducted with the process owners and processors, technology team, procurement team and other teams relevant to the Critical Operations to set initial tolerance levels.










In setting tolerance levels, the following open questions are considered:

|  Maximum period of time |  Maximum data loss |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MAO <ul style="list-style-type: none">What is maximum time of disruption before there is a material adverse impact to customers, firm and market, assuming no recovery procedures are performed? RTO <ul style="list-style-type: none">What is the desired time required for the systems and resources to be back up and running to minimise the impact to customers, firm and market? Note that this should be the desired time rather than the current capability of the systems and resources | <ul style="list-style-type: none">What is the maximum amount of data (measured in time) that the business is willing to tolerate? Additional considerations <ul style="list-style-type: none">How frequent is data backed up on the critical systems?How much data are you able to lose before significantly impacting the organisation?What is the effort required to re-key data when systems are down? |

|  Minimum service levels | | | |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none">What is the minimum service levels you will operate whilst under disruption? <p>Consider the current service levels provided to customers and other impacted stakeholders and determine what would be appropriate under severe disruptions.</p> | | | |
|  People |  Technology |  Service providers |  Facilities |
| <ul style="list-style-type: none">How many staff and what are the systems, service providers and sites required during a disruption for services to resume operating at minimum service levels? In answering the above questions, the following should also be considered <ul style="list-style-type: none">Ability and time required to bring additional people from other business areas to help process the backlogHistorical data on customer complaints especially in the event of disruptionAbility to work from homeRequired access to the facilities to keep the Critical Operation runningThe ability to perform activities in-house on behalf of the service providers | | | |

Example of a potential Tolerance Setting Output for Unit Pricing.

ACSA Members will set their own tolerance levels – this is illustrative only

| |  Max time outage |  Max data loss |  Minimum service levels | | | | |
|---------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | | | |  People |  Technology |  Service providers |  Facilities |
|  Unit pricing | MAO – 48 hours (2 NAV cycles) | 24 hours | Publish NAVs or unit prices on a daily basis on a go forward basis. Catch-up pricing will occur once minimum service levels have been achieved. | The fund accounting target operating model split is 20% onshore to 80% offshore. Critical operations would assume a minimum of 50% of people available to meet key deliverables. | Market reference data Reconciliations Fund accounting Trade processing Corporate actions processing Workflow and oversight Reporting | Third party registry Market reference data SaaS vendors Outsource vendors Third party market data service recipients | Facilities for people and technology are located in multiple locations globally Business Continuity sites in same country. Technology applications for production and business continuity are located in different countries. |
|  Justification | MAO – In the event Fund Accounting cannot process a Net Asset Value (NAV), the Client will instruct the transfer agent of the approach to be taken under their scenario testing to mitigate / manage the risk. Funds not being priced for a number of NAV cycles, i.e. distribution periods are typically not considered outside MAO in a business as usual (BAU) environment. | The longest duration of data loss for any application in the critical operation process is 24 hours. The majority of critical applications have data loss under 4 hours. Applications with a hot backup would also have batch driven recovery if the production and hot backup were compromised. | Deliver the minimum service level at 24 hours plus the invoke the RTO in the event of a severe disruption Minimum service level plans and runbook documented to achieve the objective. Scenario testing of severe but plausible disruptions undertaken periodically to enhance preparedness. Disruption events may not be isolated to just Custodians e.g. network, power grid failures, Microsoft , etc. | Resources in multiple countries to operate critical and non-critical operations. Focus on critical operations will divert resources from non-critical operations, shift work, follow the sun operating model and overtime. Minimum service levels would expect to increase over time to normal BAU levels (e.g. pandemic, natural disaster etc) | Analysis of the associated metadata has been undertaken to detail how the process is operated from an Operating Model and Technology infrastructure view. Each application has been reviewed to determine the MAO, RPO and RTO that forms part of the Tolerance Setting objective. Location of the production and business continuity sites. | Register of service providers include vendor owned (SaaS), market reference data providers, third parties that are providers or recipients of data. Minimum service levels forms part of the reviews undertaken in determining the MAO, RPO and RTO. Where a service can be run in-house in the event of an outage of a service provider it will be wherever possible. Where market reference data providers are unable to meet their obligations, there are secondary and tertiary pricing sources that will be defaulted to. | The relative criticality of business activities along with clearly defined recovery requirements, various strategies are employed to ensure operational resilience and sustainability while in business continuity. This would be a combination of relocation to business continuity recovery sites or working remotely. This was successfully demonstrated during the COVID-19 pandemic. |

Information Classification: General

Commencement of CPS 230

ACSA members recognise that upon the commencement of CPS 230 they will need to provide their APRA regulated clients with additional transparency over those critical operations and operational resilience tolerances that in turn support client related critical operations, the overall risk management framework, approach to business continuity and how service providers are monitored and overseen.

Custodians all have different operating models and risk assurance frameworks which are not standardised across every custodian.

Key Considerations for APRA Regulated Entities

- Their own approach to establishing tolerances having regard to their critical operations and impact on members/clients in the event of disruption
- Obtaining an understanding of the custodians critical operations relative to the custodial services provided and how these intersect with and/or support a critical operation of the APRA regulated entity
- Ongoing engagement with their custodian as critical operations and associated tolerances are refined over time.
- The approach to vulnerability management (including their own alternative arrangements) where gaps are identified.
- The needs and implications of any scenario based testing with their service provider including assessment of results and potential impact on their ability to remain within tolerance for their own critical operations

Glossary of Terms

BAU – Business As Usual

BIA – Business Impact Analysis

BCPs – Business Continuity Plans

Critical operations¹ - Critical operations are processes undertaken by an APRA-regulated entity or its service provider(s) which, if disrupted beyond tolerance levels, would have a material adverse impact on depositors, policyholders, beneficiaries or other customers, or its role in the financial system. It is the responsibility of an APRA-regulated entity to identify its critical operations. APRA does not expect entities to rely solely on the list of activities prescribed by APRA as critical operations.

Fourth Party² - service providers may, in turn, rely on other service providers (fourth parties). A fourth party is a party that a service provider relies on in delivering services to an ARE. APRA expects that an entity would be aware of, and manage, the risks associated with fourth party and other downstream service providers for critical operations, including the correlated risk that arises when several of its service providers are reliant on the same fourth party.

Tolerance levels³ - for each critical operation, an APRA-regulated entity must establish tolerance levels for:

- the maximum period of time the entity would tolerate a disruption to the operation
- the maximum extent of data loss the entity would accept because of a disruption; and
- minimum service levels the entity would maintain while operating under alternative arrangements during a disruption

MAO – Maximum allowable outages: The maximum amount of time a business service can be unavailable before the impact is deemed unacceptable

Material service provider(s)/Material arrangements⁴ - material service providers are those on which the entity relies to undertake a critical operation or that expose it to material operational risk. Material arrangements are those on which the entity relies to undertake a critical operation or that expose it to material operational risk. 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 or multiple arrangements with an APRA-regulated entity. 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:

- for an ADI: credit assessment, funding and liquidity management and mortgage brokerage
- for an insurer: 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

[1] Paragraph 35 of the final CPS 230 rules

[2] Paragraph 48c of the final CPS 230 rules

[3] Paragraph 38 of the final CPS 230 rules

[4] Paragraph 49 and 50 of the final CPS 230 rules

Glossary of Terms

Material offshoring arrangement⁵ - a material arrangement where the service provided is undertaken outside Australia. Offshoring includes arrangements where the service provider is incorporated in Australia, however, the physical location of the service being provided is undertaken outside Australia. Offshoring does not include arrangements where the physical location of a service is performed within Australia if the service provider is not incorporated in Australia.

RLO – Recovery level objective: The minimum service levels under alternative arrangements

RPO – Recovery point objective: The maximum amount of data loss that the business can tolerate in terms of time

RTOs – Recovery time objectives: The maximum amount of time allowed for the recovery of information assets that relate to a business service

[5] Paragraph 59b of the final CPS 230 rules

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

Important Note

ACSA works with peer associations, regulators, and other market participants on a pre-competitive basis to encourage standards, promote consistency, market reform and operating efficiency. The views expressed in this paper are prepared by ACSA and should not be regarded as the views of any particular member of ACSA.

While care has been taken in preparing this material, ACSA do not warrant or represent that the information, recommendations, opinions or conclusions contained in this document ("Information") are accurate, reliable, complete or current.

To the extent permissible by law, ACSA shall not be liable for any errors, omissions, defects or misrepresentations in the Information or for any loss or damage suffered by persons who use or rely on such Information (including by reasons of negligence, negligent misstatement or otherwise).

The comments in this paper do not comprise financial, legal, regulatory or taxation advice.



CPS 230 OPERATIONAL RISK