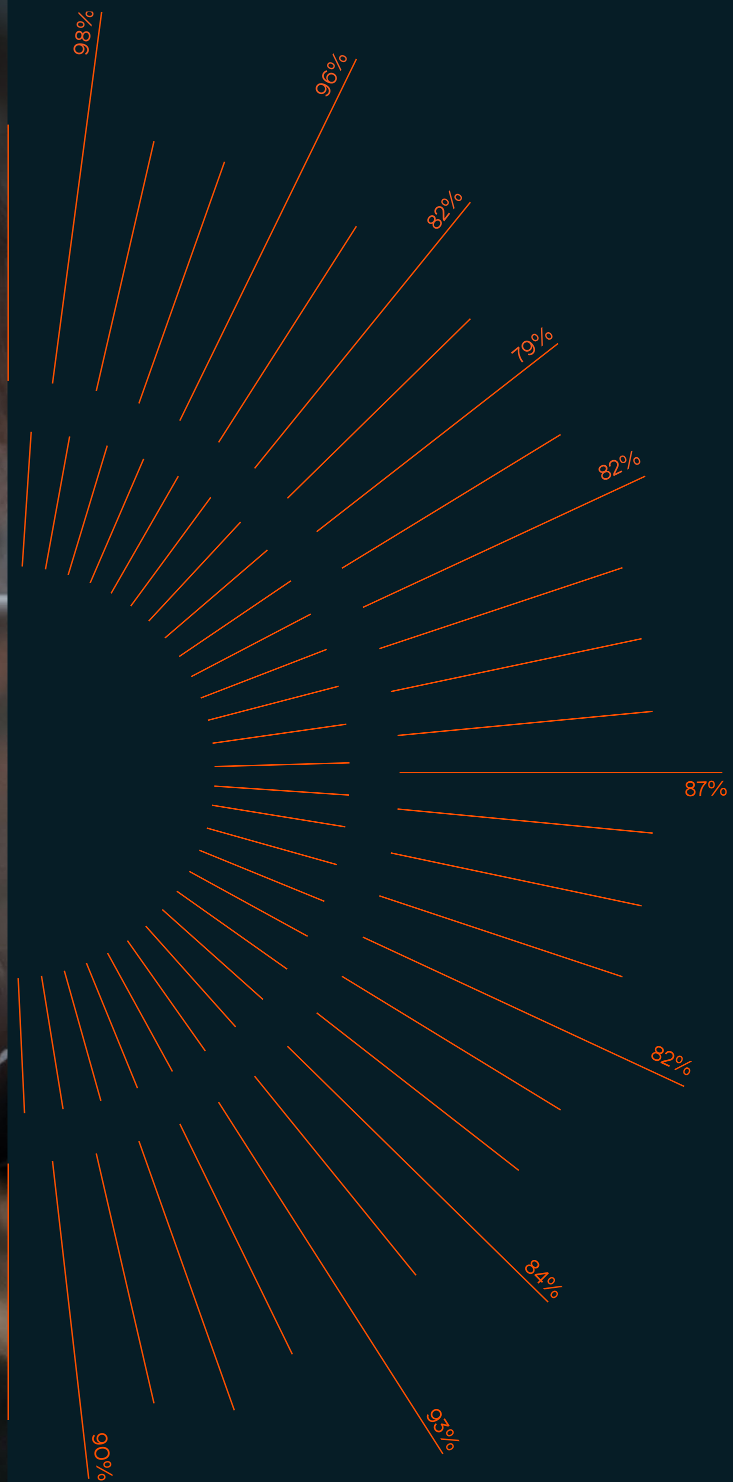
Operational Resilience



APRA's new Prudential Standard CPS 230 for Operational Risk Management comes into effect on 1 July 2025

DROVA

Contents

Not if, but when:
Disruption is inevitable 3

New APRA Standards
CPS 230 01/01/25 5

3 Pillars of CPS 230 6

01 Pillar 1:
Operational risk management

Critical Operations,
Processes & Resources 7

Impact Tolerances 9

Scenario Testing 10

Reporting 11

02 Pillar 2:
Business continuity planning

Business Continuity Planning
(BCP) 12

03 Pillar 3:
Service provider management

Service Provider Management 13

Not if, but when: Disruption is inevitable

Multimillion dollar data breaches. Pandemics. Devastating weather events. The war in Ukraine. Climate change. Cybersecurity & economic disruptions… to name a few.

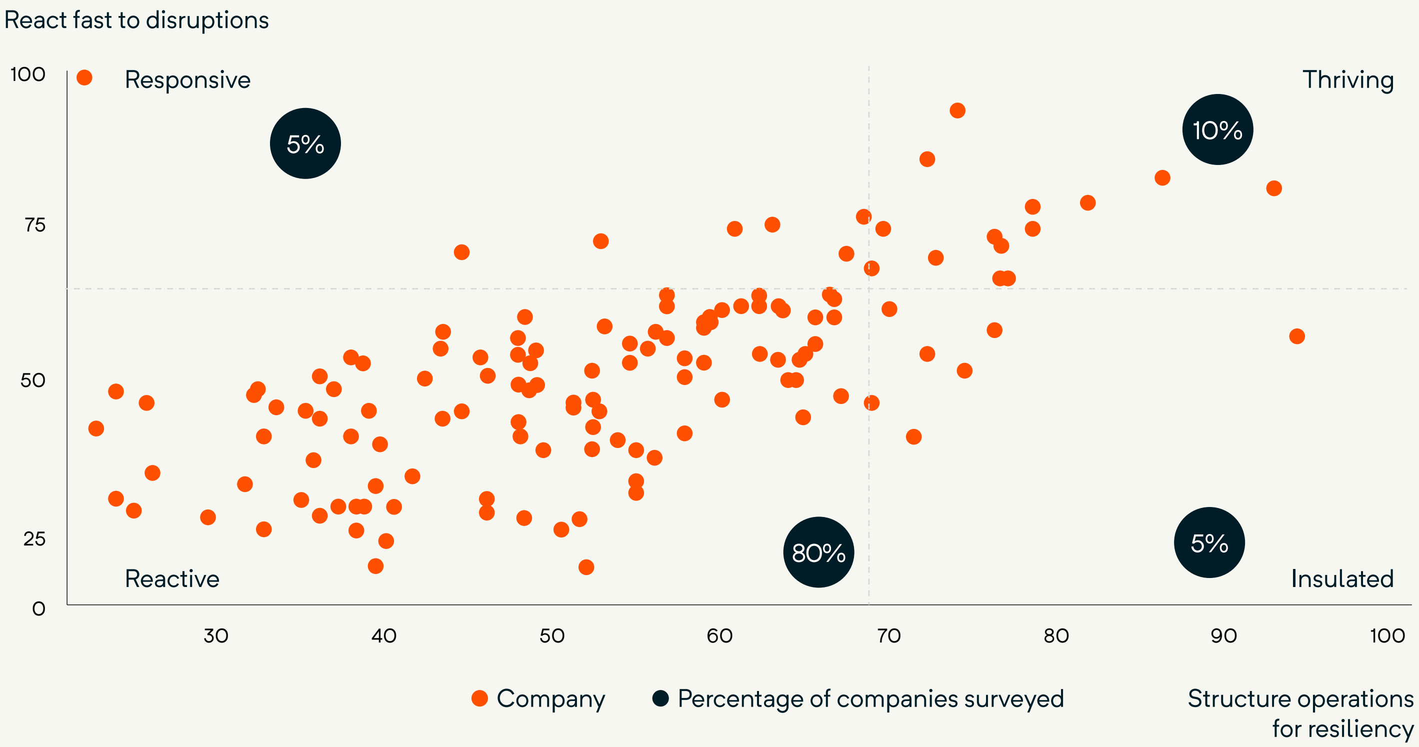
It's not a case of 'if' disruption might happen, but when. And most companies simply aren't prepared. Data shows that only 10% are resilient and thriving.

When any disruption occurs that impacts operations, companies must be able to respond quickly and well. They may have to accelerate their digital transformation, make real-time decisions, and pivot their operational practices rapidly.

This is Operational Resilience. It's critical for all businesses, and it's a critical component of a modern GRC framework.

That's why the Australian Prudential Regulation Authority (APRA) has finalised a new prudential standard for insurers, banks and superannuation firms – CPS 230 Operational Risk Management – to ensure they better manage operational risks and business disruptions.

Only 10% of companies are truly resilient and thriving



60%

A study by Deloitte showed that 60% of organisations have experienced a disruptive incident in the past two years

53%

A 2021 CDP report showed that over half of suppliers experienced climate-related disruptions in their supply chains the previous year

$75m

A 2020 study by the Ponemon Institute showed that 53% of organisations experienced a data breach caused by a third-party, costing $7.5 million on average to remediate

New APRA Standards CPS 230 01/01/25

The proposed new standard for operational risk management, which will replace and supersede a number of existing standards in this area, encompasses operational risk controls and monitoring, business continuity planning and the management of third-party service providers.

What will it replace?

The proposed Prudential Standard CPS 230 Operational Risk Management (CPS 230) will replace five existing standards:

Prudential Standard CPS 231 Outsourcing (CPS 231) and Prudential Standard CPS 232 Business Continuity Management (CPS 232) that apply to ADIs, life insurers and general insurers, the equivalent superannuation standards.

Prudential Standard SPS 231 Outsourcing (SPS 231) and Prudential Standard SPS 232 Business Continuity Management (SPS 232) and the private health insurance standard Prudential Standard HPS 231 Outsourcing (HPS 231).

Who will be affected?

The rules will affect authorised deposit taking institutions (ADIs), general insurers, life insurance, private health insurers and Superannuation Entities. It will include firms and entities authorised and registered under the Banking Act, Insurance Act, Life Insurance Act, PHIPS Act and the SIS Act.

Objectives:

Improve operational risk practices through enhanced focus of Boards and senior management

Minimise the impact of disruptions to customers and the financial system

Key features:

- Entities must manage operational risks with effective internal controls, monitoring and remediation
- Entities must be able to respond to disruptions and maintain continuity of critical operations
- Entities must understand and manage risks from the use of service providers
- Entities must now report on certain events and relationships with service providers

Information sourced from: https://www.apra.gov.au/discussion-paper-strengthening-operational-risk-management

3 Pillars of CPS 230

Operational Resilience

Operational Risk Management	Business Continuity Planning (BCP)	Service Provider Management
Effectively manage operational risks	**Maintain critical operations through disruptions**	**Manage the risks associated with service providers**
Important Business Services, Critical Processes & Resources	Register of critical processes and their tolerance levels	Comprehensive service provider management policy
Impact Tolerance	Ongoing audits & reviews	Identification of material service providers
Scenario Testing	Triggers to activate BCP in face of disruption	Risk management of material service providers
Reporting		

Critical Operations, Processes & Resources

Stage 1 is identifying your critical operations (also known as Important Business Services) and mapping out the processes and resources that support them.

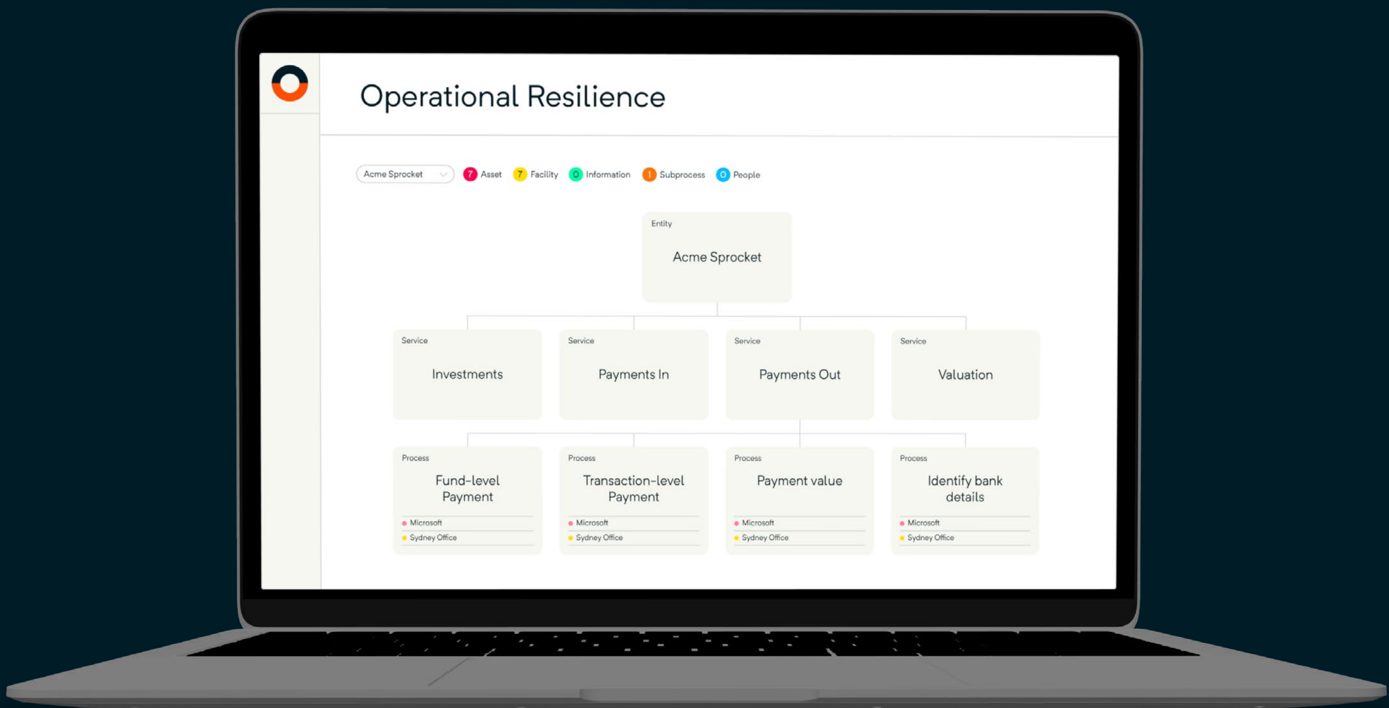
What services are crucial to maintain operations? What processes, systems, people, data or third parties support these services?

The Operational Resilience module uses AI to quickly generate a selection of business services most relevant to your organisation. Edit these as a template or add your own.

For each important service, break down critical processes into the resources that support them, mapping each process flow to understand its conditions and resource dependencies.

Use Drova to:

- Create a centralised and accessible register of critical services
- Assign these to stakeholders and rate their priority & criticality
- Understand and maintain critical operations to minimise the likelihood and impact of disruption
- Link services to other records throughout the GRC system, enabling links to third parties, time-based metrics, risks, events and scenarios
- Ensure the resources that enable critical services and processes can adapt in the event of disruption
- Set alternate processes or resources where a disruption occurs



Impact Tolerances

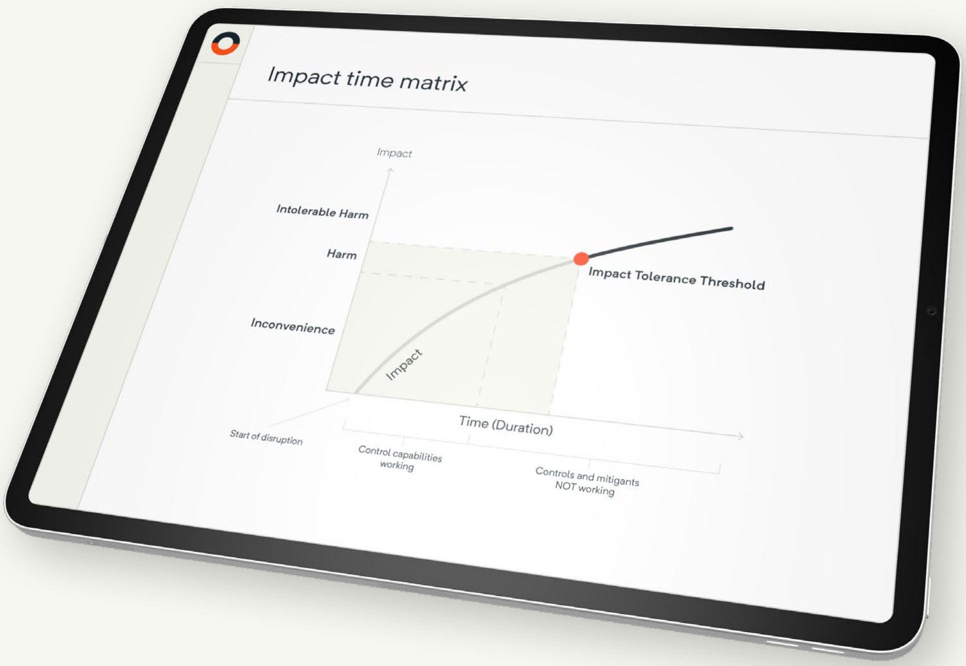
Stage 2 is setting clear impact tolerances for the maximum level of disruption you are willing to accept, including around data loss.

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

- (a) the maximum period of time the entity would tolerate a disruption to the operation;
- (b) the maximum extent of data loss the entity would accept as a result of a disruption; and
- (c) minimum service levels the entity would maintain while operating under alternative arrangements during a disruption.

Use Drova to:

- Define what is an 'inconvenience' vs. 'intolerable harm', and establish tolerance levels across processes and resources
- Use the Impact Time Matrix to measure the impact against the duration the service is not working
- Put in controls and mitigants to ensure you can maintain critical operations within tolerance levels
- Be able to confidently demonstrate this to APRA
- Once tolerances are established, conduct regular scenario testing to calibrate impact tolerances



Scenario Testing

Stage 3 requires conducting scenario testing, using severe but plausible scenarios to assess your ability to remain within your defined impact tolerances.

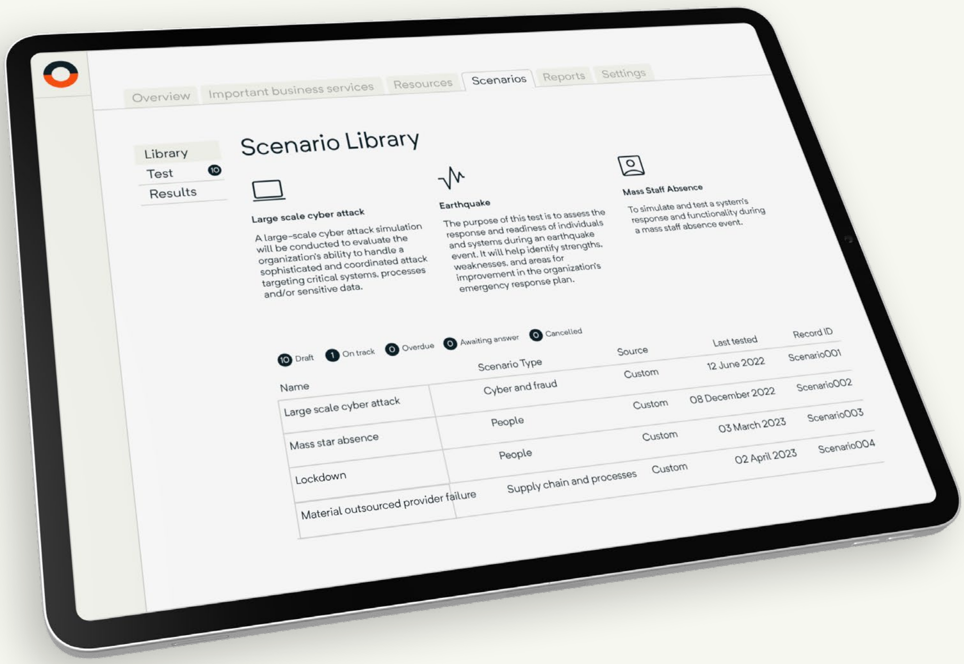
How would a disruptive event impact your most important processes? What happens next?

Tests should include failures within your control (e.g. IT system failures) as well as those outside of your control (e.g. cyber attack or disruption to power supply).

Every sector and organisation will be different. Find drivers, triggers and other factors to inspire useful scenarios in our AI-powered Scenario Library, which includes any mandatory testing required or suggested by APRA.

Use Drova to:

- Access a library of suggested scenarios
- Guided scenario tests are set up for you to execute at the click of a button
- View the results of your tests and how they stack up against your impact tolerances
- Measure your tolerance across a specific duration and see how long recovery would take to ensure that you are not crossing into 'intolerable harm' levels
- Maintain a detailed audit trail of all your scenario tests in the centralised platform, including results, tests completed and tests approved



Reporting

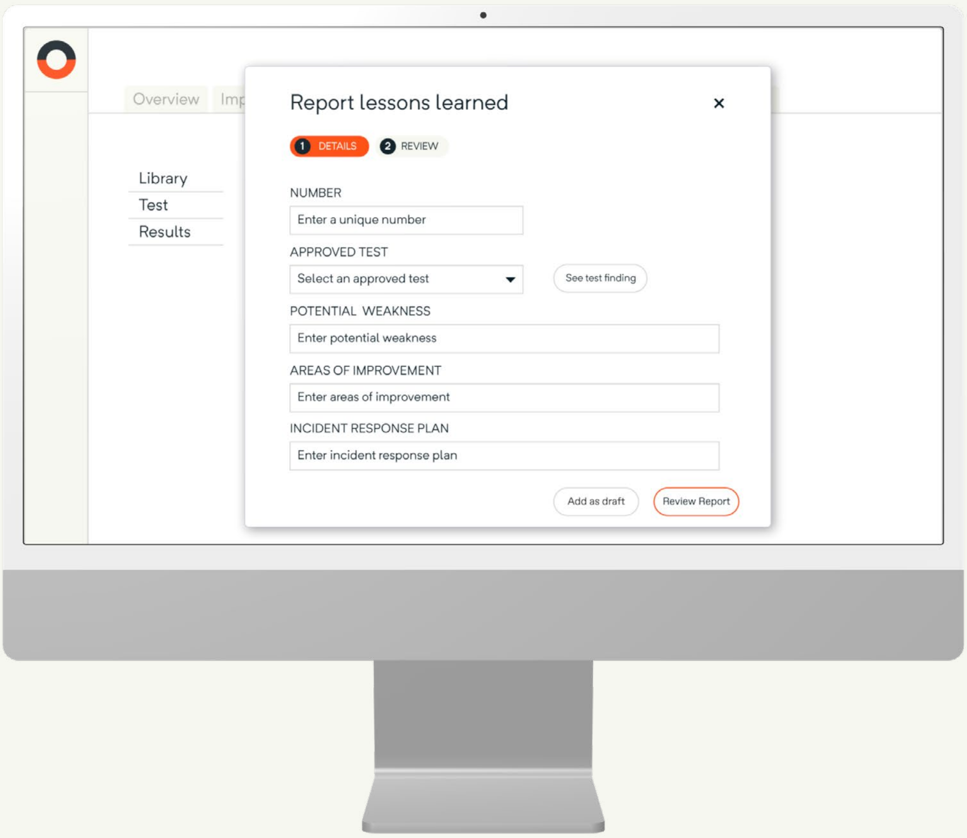
Stage 4 requires developing and maintaining appropriate monitoring, analysis and reporting of operational risks and escalation processes for operational incidents and events.

This includes the use of effective information systems to monitor operational risk, compile and analyse data, and facilitate reporting to the Board and senior management.

The Board must also approve the service provider management policy through the review of risk & performance reporting on material service providers. Your internal audit function must also regularly report to the Board on compliance with this policy, and review any arrangement involving the outsourcing of a critical operation.

Coming soon:

- Align with APRA reporting standards
- Produce professional executive and Board reporting for visibility across your organisation
- Give APRA and auditors a clear and holistic view of your critical operations and the processes and resources mapped to them



Business Continuity Planning (BCP)

APRA-regulated firms must have BCPs in place that outline how the firm identifies, manages, and responds to disruptions within tolerance levels. These BCPs must be regularly tested with severe but plausible scenarios.

BCPs must include Disaster Recovery (DR) planning for critical information assets, ready to be activated during a disruption before returning to normal operations.

Firms must maintain the necessary capabilities to execute the BCP, including access to people, resources and technology. Ultimately, the Board is responsible for overseeing BCPs as part of overall risk management.

Use Drova to:

- Map critical processes and contingencies to allow for integrated BCP testing
- Identify resources (people, information, assets, third-party suppliers) for BCP testing and oversight
- Provide the Board an inside-out (business critical process) to plausible scenario analysis view of BCP operations and capabilities
- Operational resilience task management provides required systematic testing program, tailored to material risks
- Establish governance via assigned roles and responsibilities

Service Provider Management

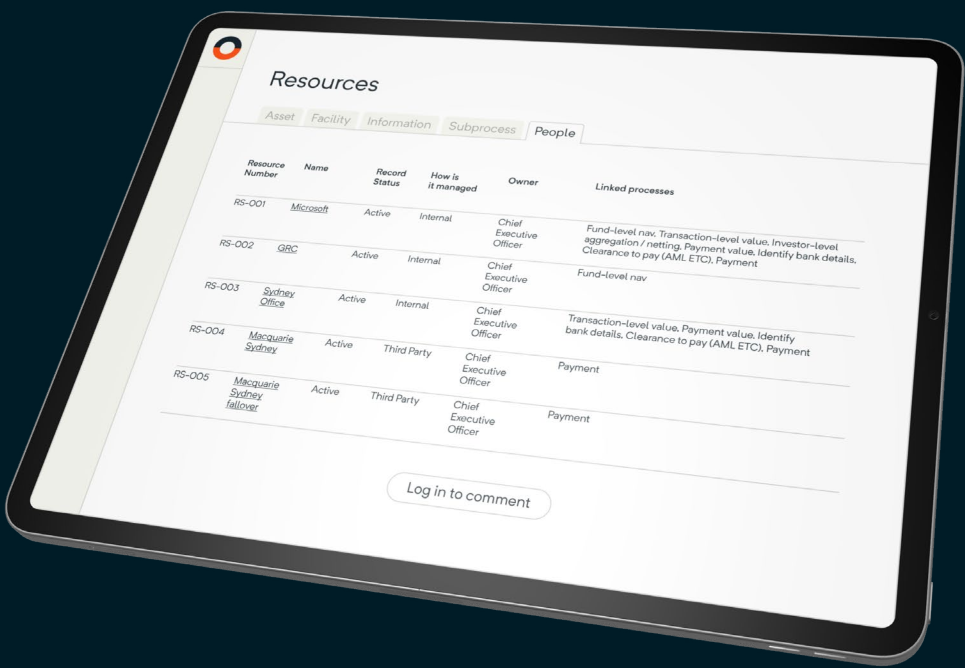
Under CPS 230, firms must maintain a register of material service providers and manage risks associated with them. Regularly monitor material arrangements, assess performance, evaluate risk controls, and ensure compliance with the service provider agreement.

The register of material service providers must be submitted to APRA on an annual basis, with senior management also receiving regular reporting.

APRA needs to be notified within 20 days of entering or significantly changing an agreement for a service critical to operations. They may also request changes to an agreement if heightened prudential concerns are identified.

Use Drova to:

- Track and identify all third-party resources (assets, facilities) that enable your critical operations
- Maintain a register of your material service providers and manage all contracts with third parties in the centralised platform
- Conduct attestations and due diligence on service providers
- Maintain visibility and manage financial and non-financial risks by linking your service provider contracts to your risk and compliance records
- Test resources managed by service providers through integrated scenario testing



To effectively navigate disruption today, businesses must shift from a traditional risk management approach to a comprehensive assessment of operational resilience. CPS 230 can offer risk managers and the Board a profound understanding of their organisation's internal and external resilience and risk landscape.

Operational resilience spans critical aspects including cyber threats, third and fourth-party resilience, climate resilience and more, forming a foundational framework for addressing modern business challenges.

Drova provides a complete Governance, Risk and Compliance solution, integrating all facets of operational resilience. Our platform covers risk management, control assessment, event tracking, contract management, policy compliance, regulatory scanning and more.

It not only maps critical processes, but also enhances visibility into third-party resources, supply chains, digital assets, and cybersecurity.

Operational resilience, with its value chain analysis and climate resilience scenarios, lays the groundwork for compliance with emerging ESG legislation like ISSB S1, S2, and CSRD requirements.

Drova is your partner on the journey toward ESG excellence, ensuring your operational resilience aligns seamlessly with evolving regulations, shaping a sustainable and resilient future for your organisation. Where does your organisation stand on ESG today?

Learn more about Drova for operational resilience.

Try now for free

Drova is a SaaS software platform that delivers solutions for GRC, resilience and sustainability management. Our vision is to enable every company to thrive by putting sustainability and resilience at the heart of their success.

We're on a mission to create technology that helps companies drive impact through innovation, bring their people along for the journey, and ultimately create long-lasting value.

We are here to ignite the potential within every organisation by embedding sustainability and resilience into their strategy and operations, making these the cornerstones of every success story.

Learn more at drova.com

DROVA

drova.com