Operational Resilience: Super in focus

Prudential Standard CPS 230

March 2023
Consolidation can create operational risk for super funds

Australian superannuation institutions are undergoing consolidation due to pressures on performance, fees and sustainability. This pressure is also felt by their service providers who themselves have also consolidated in key areas such as administration, custody and insurance as they seek to scale, reduce costs and to meet the needs of superannuation funds.

Consolidation can lead to concentration risk and transition risk as providers exit the market (e.g. in Custody, Insurance and Administration). If not appropriately understood and managed (especially for critical operations) this can cause an intolerable level of harm to members, the viability of the fund and/or the stability of the superannuation sector.

To succeed on the CPS 230 journey, it is important that the requirements are not considered in silos and board accountabilities are supplemented with clearly delegated responsibilities to support a comprehensive end-to-end mapping of critical operations. With the interconnectedness of other future regulatory requirements such as the Financial Accountability Regime (FAR), Operational Risk Financial Requirement (consultation on SPS 114), Recovery and exit planning (CPS 190), member outcomes and transfer planning, superannuation funds should ensure the approach is consistent and integrated.

Getting this right requires mapping and implementing an effective enterprise wide controls framework to mitigate the suite of operational risks.

What do funds need to do?

The Board is responsible for operational risk management and oversees management’s implementation and maintenance of CPS 230. This includes internal controls and approving tolerance levels for critical operations.

The Board must approve the service provider management policy and supervise the performance of service providers.

Operational Risk Management

To support a comprehensive Operational Risk Profile and Business Continuity Plan (BCP), Entities must understand their critical operations and minimise the likelihood and impact of disruption as part of their business continuity planning. This includes identifying the resources and interdependencies that can be disrupted (e.g. people, technology, information, facilities and service providers).

Entities must review and update (where applicable) its Operational Risk Profile. This includes the implementation of internal controls to mitigate risks within appetite and meet obligations, which should be embedded and regularly tested. Entities must also maintain a strong data and Information Technology (IT) infrastructure to meet business requirements and support critical operations.

Entities must establish Board-approved tolerances for the maximum level of disruption they are willing to accept, including around data loss. Impact tolerance levels set need to be member outcomes-focused.

Service provider management

Entities must understand and manage the risks associated with the use of the service providers that support their critical operations or expose them to material operational risk, including downstream providers (fourth parties).

A register of MSPs and associated risks must be reported to APRA annually, as well as changes to MSP agreements.
CPS 230 in practice: Benefits processing

To support a comprehensive Operational Risk Profile and an appropriate corresponding Business Continuity Plan, the Board must understand critical operations across the organisation. This is supported by a detailed end-to-end mapping of each critical operation including their enablers such as technology and material third party Service Providers. The identification and implementation of effective key controls which support the appropriate management of operational risk is key in this process. The below illustration summarises the key considerations for superannuation funds by using “Benefits processing” as an example.

### Operational Risk Management

- Identify and document the key operational risks across its critical operations for example the handovers between different providers, lack of understanding of technology & cyber risks, unclear roles & responsibilities which may lead to human errors when processing payments.
- Document key controls across each risk with identified accountable owners.
- Identify opportunities to uplift and implement changes to the current risk appetite and escalation thresholds relative to critical operations.
- Identify changes required to operational risk profiles, including obligations and controls and identifying the necessary amendments.
- Assess whether the information technology infrastructure to support critical operations are being maintained for example the online forms from the fund-managed website.
- Implement processes to identify, monitor, report and escalate operational risk incidents and near misses (to the Board and to APRA).

### Business Continuity Management

- Set tolerance thresholds for each component of the ‘severe but plausible’ scenario. Consider the different intervals throughout the year for example, the criticality of processing contributions in March vs at 30 June, in terms of tax consequences for members will be different.
- For tolerable levels of disruption to members, not all payments may be considered critical, but some will be e.g. pension payments.
- Update/ Develop Business Continuity Plan for the identified critical operation.
- Monitor and report non-compliance with tolerance levels.
- Business led periodic testing (at least annually) to ensure the ‘severe but plausible’ scenarios are current, and the BCP remains effective.

### Service Provider Management

- Review the end-to-end critical operations to identify dependencies on service providers that were not necessarily considered material outsourced providers in the past for example, banking portals. These were not generally considered a material outsourced provider but they do facilitate money out (payments) which is a critical operation.
- Identify and record material service providers (There could be service providers that are not APRA-regulated – including some custodians. Consider service providers whose jurisdictions is outside of Australia where the regulatory requirements differ to APRA’s).
- Conduct due diligence with material service providers before entering into new arrangements, or renew and/ or change existing arrangements to meet minimum APRA requirements.
- Identify the key financial and non-financial risks for each material third party service provider. Map associated risks and implement appropriate controls.

### Governance & Oversight

- Establish clear Governance & Accountability, including defined responsibilities. The Board is primarily responsible for operational risk management and must oversee senior management’s implementation and maintenance of CPS 230.
- Update Risk Management Framework to reflect updated policies and standards.
- Independent Assurance over the credibility of the organisation’s Business Continuity Plan (BCP) as well as its compliance with the Service Provider Management policy.

### How can we help?

- CPS 230 readiness review, maturity and benchmarking assessment.
- Operational resilience Target Operating Model (TOM) design.
- Operational resilience program planning, scoping and delivery.
- Operational resilience governance (incl. framework development) and accountabilities identification.
- Board and executive awareness sessions.
- Critical operations definition and documentation, including resources.
- Internal controls mapping, across the identified risks and obligations.
- Operational risk profiling (incl. risk appetite update).
- Operational resilience review to identify potential resilience gaps in the environment.
- Controls assurance (incl. gap identification and remediation action).
- Impact tolerance identification.
- Business Continuity and Disaster Recovery Planning.
- Training and awareness.
- Scenario testing.
- Material service provider (MSP) assessments.
- Third Party Risk Management Framework.
- Third party controls testing (for MSPs).

### Contacts

- **Peter Malan**
  - Partner
  - Cybersecurity & Digital Trust
  - T: +61 413 745 343
  - E: peter.malan@pwc.com

- **Carley Bryce**
  - Partner
  - Risk & Controls
  - T: +61 412 929 373
  - E: carley.bryce@pwc.com

- **Nathan Bonarius**
  - Partner
  - Superannuation
  - T: +61 487 887 474
  - E: nathan.bonarius@pwc.com

- **Susanna Chan**
  - Partner
  - Operational Resilience
  - T: +61 414 544 066
  - E: susanna.chan@pwc.com
Thank you