CPS 230

FOCUS AREAS FOR COMPLIANCE WITH THE NEW STANDARD

This document assumes present compliance with **CPS 220 Risk Management** | **CPS 231 Outsourcing** | **CPS 232 Business Continuity Management**

Amstelveen

Operational Risk Management

In addition to the requirements of CPS 220 Risk Management, regulated entities should:

Ensure the Operational Risk Profile, including risk indicators, control effectiveness and major incidents/issues are communicated to the Board efficiently.

Update the Risk Appetite Statement, Risk Management Strategy, Risk Taxonomy and other framework documents to ensure operational risk is sufficiently covered.

Review and uplift (or implement) processes for:

- Risk in change
- Material customer onboarding
- Control assessment (to include design and operating effectiveness)
- Issue management
- Incident management
- Scenario analysis to include severe but plausible operational risk events

Document and map processes, risks, controls and required dependencies for critical operations. Ensure active engagement of line management.

Update (or implement) Integrated Risk Management systems to support the above processes and operational risk data and ensure data quality is managed and insights reported effectively.

Amstelveen

Business Continuity Management

In addition to the requirements of the soon to be superseded CPS 232 Business Continuity Management, regulated entities should:

Update the Business Impact Analysis approach to ensure critical operations are aligned with those prescribed by APRA and capture Maximum Tolerable Period of Disruption, Maximum Tolerable Data Loss and Minimum Business Continuity Objective for each. The BIA should align with, or be, the source of truth for “critical operations”.

Ensure the Business Continuity Plan(s) include new requirements for activation triggers and procedures, execution risks, dependencies and a process for notifying APRA within 24 hours of activation.

Seek Board approval of the Business Impact Analysis for critical operations and Business Continuity Plan(s) initially and in future on refresh at least annually. The BCP will also need to be submitted to APRA.

Ensure there is alignment and integration between BCM processes and registers, including the “critical operations” register, “material service providers” register, supplier contingency plans and operational risk requirements to ensure that the likelihood and impact of disruptions is minimised in a coordinated way.

Conduct multi-year BCP test planning to ensure testing cycles through various relevant scenarios over time, including disruption to material service providers. Ensure test results are periodically reported to the Board.

Amstelveen

Service Provider Management

In addition to the requirements of the soon to be superseded CPS 231 Outsourcing, regulated entities should:

Update their Outsourcing Policy to a Service Provider Management Policy which meets the updated requirements. There may be an opportunity to consolidate different policies as part of this (e.g. procurement, supplier governance etc).

Update the frameworks/processes for assessing the risk and materiality of arrangements in line with the new requirements, and ensure this is embedded within the existing procurement and supplier onboarding and renewal processes

Review all existing arrangements in the context of the updated materiality assessment, and uplift those now deemed material on contract renewal (or earlier).

Update standard contract templates and gap assess existing material contracts against the new requirements to determine where contractual uplift is required.

Ensure any reliance on related bodies corporate for critical operations is reviewed in the context of the new requirements – these are to be treated the same as regular service providers with a legally binding agreement in place.

Define and implement a process for managing fourth party risk.

Review processes for monitoring service providers and ensure that it includes reporting to senior management on control effectiveness and contractual compliance (as well as performance). Monitoring should also consider risks, contingencies and business continuity on an ongoing basis.

Ensure there is a register of material service providers in place, which must be submitted to APRA on an annual basis.

Amstelveen

Amstelveen equips organisations to identify, assess and mitigate their most significant risks. Our risk, compliance and technology professionals support clients to improve the governance of their organisations. We provide specialist support to the largest public and private organisations in Australia and New Zealand.

Amstelveen