Feedback on Table 7 Questions

Table 7. Key questions

Overall design	1. Is a single cross-industry standard for operational risk management supported? 2. Are there specific topics or areas on which guidance would be particularly useful to assist in implementation? 3. How could proportionality be enhanced in the standard, and is there any merit in different requirements for SFIs and non-SFIs? 4. What are the estimated compliance costs and impacts to meet the new and enhanced requirements?
Specific requirements	1. How could APRA improve the definitions of critical operations, tolerance levels and material service providers? 2. What additions or amendments should be made to the lists of specified critical operations and material service providers? 3. Are the notification requirements and the time periods reasonable? 4. What form of transition arrangements and timeframe would be needed to renegotiate contracts with existing service providers (if required)?

Overall Design

See below text bolded in yellow for our recommendations for APRA's consideration.

Feedback on Question 2 – Are there specific topics or areas on which guidance would be particularly useful to assist in implementation?

1. PROGRAM VERSUS PROJECT

We have found that the focus and energy devoted to business continuity is often sporadic and dependent on the focus on one senior executive.

The market in Australia is relatively immature and there is a large variation in how thoroughly this discipline is practised. We believe that a major impediment is that often these initiatives are not supported by a business case. When it comes to budget time, the development and operation of a business resilience program loses out to better justified programs, resulting in insufficient funds being allocated in the budget.

We recommend to our clients that these initiatives should be:

- Considered as programs that span multiple financial years and that need to be improved over time.
- Have strong executive sponsorship.
- Be embedded into the organisation.
- Be reviewed annually.

2. GOVERNANCE

APRA rightly requires that the Board have oversight and ultimate responsibility for these activities.

We have found that governance arrangements have not been explicitly put in place. We recommend to clients that the following governance arrangements be established for these two situations:

- BAU – development and exercising the program, funding, improvement over time, meeting regulatory obligations etc
- Crisis Management – when things go wrong, the entity's Crisis Management Team is stood up to manage any crisis. It is imperative that the CMT be comprised of the CEO and the senior leadership team and that they have the delegated authority to make decisions on behalf of the entity. The CMT's role is to make the big decisions, approve communications and keep the Board apprised.

Clause 15(a) makes mention of governance arrangements. Should governance receive more attention in CPS 230?

3. SINGLE POINTS OF FAILURE

As part of the implementation of a program, we review the client's Risk Assessment. We often find that:

- It has been completed in the absence of a Board approved Risk Appetite.
- It pays inadequate attention to Single Points of Failure (SPOF).
- It pays inadequate attention to third party risks – especially from cloud providers and global supply chain.

There is no mention of SPOF in CPS 230. Should specific mention be made of the risks presented – especially post COVID and the ensuing supply chain issues we have suffered?

4. SEMANTICS

We strongly advocate against the use of the word "Testing" for the following reasons:

- It infers a Pass or Fail. This can sometimes lead to participants not being totally candid during testing and post exercise reviews.
- We advise clients that skills should be improved over time through regular exercising, not by a pass or fail of test.
- The point of an exercise is to uncover faults or weaknesses. Referring to it as a test works against this objective.

Our recommendation is to avoid the use of the word Testing.

Specific Requirements

Feedback on Question 1.

5. TOLERANCE LEVELS

We are very supportive APRA's definition of Tolerance Levels. They are more understandable (for a business person) than the current BCI and ISO terminology of Prioritised Activity and MAO. Most clients don't understand Recovery Point Objective.

However, the MAO definition refers to the disruption becoming "unacceptable", which we find helpful.

ISO/BCI definition:

Maximum Allowable Outage time	The time it would take for adverse impacts, which might arise as a result of not providing a product/service or performing an activity, to become unacceptable.

Would it be worthwhile to insert the word into the CPS 230 definition?

The maximum period of time an entity would tolerate a disruption to the operation before its impact becomes unacceptable.

6. WHO IS IMPACTED?

We support APRA's more reasonable approach (see below) to having the entity determine the impact of a disruption to its activities, rather than the FCA's [1] approach. We believe that the FCA's approach will be very difficult to implement.

APRA has struck the right balance with the clause below.

> The setting of tolerance levels is intended to be customer and outcomes-focussed; it is these factors that an entity would be expected to have front-of-mind when determining tolerance levels for critical operations. APRA may also set tolerance levels in circumstances where there are heightened risks or material weaknesses, including at a system level.[8]

[1] UK Financial Conduct Authority - Building operational resilience: impact tolerances for important business services and feedback to DP18/04

Feedback on CPS 230

7. SCOPE OF BCP

We often find that the BCP developed by organisations omit to include detailed Recovery Procedures for each of the critical business activities and their supporting resources. These Procedures are onerous to write and many managers have difficulty in developing them.

Would it be beneficial in CPS 230 to specifically mention the need to incorporate Recovery Procedures for critical operations into the BCP?

8. EXERCISING SCOPE

We could find no mention of a requirement for regulated entities to conduct exercises in conjunction with material service providers. This can be very challenging, but given the increasing reliance on third parties (especially cloud), should this be considered?

Should CPS 230 mention the benefit of conducting joint exercises?

9. CLAUSE 53

Should CPS 230 include a clause that requires that the regulated entity receive adequate compensation from the service provider commensurate with the impact of a disruption caused by the provider?