+61 2 8005 1265
Level 8, 299 Elizabeth St.
Sydney, NSW 2000, Australia

info@protechtgroup.com
www.protechtgroup.com

General Manager, Policy
Australian Prudential Regulation Authority
Sent to: PolicyDevelopment@apra.gov.au

21 October 2022

INTRODUCTION

The Protecht Group (Protecht) welcomes the simplification and consolidation of existing APRA standards into the draft standard CPS 230 on Operational Risk. We are submitting a response to the questions raised by APRA as a result of our enterprise risk management services provided to APRA regulated institutions.

We have laid out our response in the following manner:

- Background on Protecht and our interest in the standard
- Responses directly to selected questions posed by APRA in its discussion paper
- Comments and questions on specific paragraphs or application of the standard.

BACKGROUND ON PROTECHT

Headquartered in Sydney, Australia with offices in London and Los Angeles, Protecht provides complete risk solutions, including the world-class Protecht.ERM enterprise risk management platform as well as compliance, training and advisory services to businesses, government organisations and regulators across the world.

Protecht.ERM provides a single, interconnected platform that produces a holistic view of risk while being simple and easy to use. Protecht has helped hundreds of organisations, many of them APRA regulated, move away from spreadsheets and email to a more efficient and effective way to manage risk.

Our response is informed by our industry experience and engagement with our customers who are regulated by APRA.

PROTECHT
Redefining Risk

+61 2 8005 1265
Level 8, 299 Elizabeth St.
Sydney, NSW 2000, Australia

info@protechtgroup.com
www.protechtgroup.com

RESPONSE TO APRA'S QUESTIONS

APRA posed 8 questions in its discussion paper on the standard. Protecht has provided answers to 5 of those questions.

1. *Is a single cross-industry standard for operational risk management supported?*

   Protecht supports a single cross-industry standard for operational risk management. Where applicable, differences for specific sectors or applications can be articulated in future guidance.

2. *Are there specific topics or areas on which guidance would be particularly useful to assist in implementation?*

   We have made comments on specific paragraphs of the standard in the section below.

3. *How could proportionality be enhanced in the standard, and is there any merit in different requirements for SFIs and non-SFIs?*

   Protecht believe that the principles of the standard should be applied across all entities. This is on the basis that consumers do not distinguish between SFI's and non-SFI's, or even understand these definitions.

   Impact of disruption or risk management failures are likely to impact the end consumer in the same way for similar services, regardless of the size of the financial services firm. However we recognise that an event impacting a major bank will have more severe consequences to the broader Australian financial system than a smaller financial institution.

4. *What are the estimated compliance costs and impacts to meet the new and enhanced requirements?*

   As a supplier of risk and compliance services and software to regulated entities we expect to see an increase in demand for digitisation of manual processes associated with the principles of the standard. Maintaining business continuity plans, performing control tests

+61 2 8005 1265
Level 8, 299 Elizabeth St.
Sydney, NSW 2000, Australia

info@protechtgroup.com
www.protechtgroup.com

and increasing vendor risk management capabilities is difficult to perform in spreadsheets. As a result, regulated entities will need to continue to invest in software (implementation services and licence costs) and people to execute the requirements of the standard. Training and education will also be required on how to execute the more technical requirements of BCP, control testing and vendor risk management.

We also anticipate that the material service provider requirements may result in increased costs to industry in the following ways:

- Increased due diligence and assurance requirements for the regulated entities
- Material service providers increasing their cost to provide their services upon renewal as a result of increased regulatory burden
- Potential for some existing service providers to 'opt out' of providing services in order to avoid the regulatory burden of being classified as a material service provider, which may affect competition of the services being provided

1. *How could APRA improve the definitions of critical operations, tolerance levels and material service providers?*

Defining critical operations

We believe the principle-based definition in the standard for critical operations in paragraph 34 is sound and applaud the guidance of what are considered to be critical operations in paragraph 35. We do anticipate that APRA will provide further guidance in its proposed guidance documents. Our comments are to inform development of that further guidance.

Material adverse impacts

The definition of critical operations includes operations that would have *material adverse impact* to defined stakeholders if disrupted. We anticipate that without further guidance, there will be a large range of interpretation of *material adverse impact*. For example, should adverse impact include monetary loss or loss of assets, psychological or emotional

+61 2 8005 1265
Level 8, 299 Elizabeth St.
Sydney, NSW 2000, Australia

info@protechtgroup.com
www.protechtgroup.com

impacts, lost economic opportunities, or causing the impacted stakeholder to breach regulatory, legal or contractual obligations.

Effect of small customer bases / demographics on critical operations

Paragraph 34 includes depositors, policyholders, beneficiaries or other customers as the impacted stakeholders of any particular critical operation. Within those stakeholder groups, there are likely to be a range of customer demographics or circumstances (e.g. vulnerable customers), where the assessment of a materially adverse impact may differ between those groups. From a customer protection perspective, it seems logical that an assessment of materiality would be based on the most impacted group.

As noted earlier on proportionality, we expect that the size of a customer base should not impact on the definition of a critical operation. From a consumer perspective, financial services of one firm should be provided with the same rigour and care as another.

However, an unintended consequence of the business continuity requirements may be that regulated entities:

- Cease providing a service because it is a small percentage of the organisation's overall operations (including where it might have otherwise had an extended sunset period)
- Change products or services so they no longer appeal to particular demographics with the aim to increase tolerance level timeframes and reduce business continuity compliance costs.

We acknowledge that the current standard CPS 232 on Business Continuity Management includes at paragraph 21 "*Critical business operations are the business functions, resources and infrastructure that may, if disrupted, have a material impact on the institution's business functions, reputation, profitability, depositors and/or policyholders*" which does include an assessment impact on external customers. However, with the change in focus to external stakeholders in the new standard, it may cause regulated entities to reclassify some of their low volume operations that do not form part of current business continuity arrangements as critical operations under the new standard. As a

PROTECHT
Redefining Risk

+61 2 8005 1265
Level 8, 299 Elizabeth St.
Sydney, NSW 2000, Australia

info@protechtgroup.com
www.protechtgroup.com

result, there may be the reduction in availability of specialised services to consumers if business continuity requirements and compliance costs make it difficult for regulated entities to compete.

Listed critical operations

Paragraph 35 includes a list of operations APRA has defined as critical. We anticipate that further guidance will be welcomed to assist APRA-regulated entities understand the level of granularity at which they should capture their critical operations. This guidance will facilitate practical implementation of their business continuity and operational resilience arrangements. For example, some entities will have multiple types of payments, each with their own sets of resources and customers who will be impacted differently. Guidance on the appropriate level of granularity will allow those entities to more effectively balance operational resilience outcomes with compliance costs.

Paragraph 35 also includes in its definition of critical operations *'…the systems and infrastructure needed to support those operations'*. We suggest that this inclusion may cause confusion for regulated entities. Paragraph 25(b) of the standard includes the identification and mapping of resources needed to deliver those critical operations. Systems and infrastructure are the resources required to deliver one or more critical operations, and we recommend they should be mapped to those critical operations as per paragraph 25(b). A critical operation should be limited to a service that provides an outcome to a customer.

Tolerance levels and the entity

Paragraph 37(a) states that for each critical operation, an APRA-regulated entity must establish a tolerance level for the maximum period of time the entity would tolerate a disruption to the operation.

We note the use of the word 'entity' in paragraph 37(a), which does not seem consistent with the stakeholders contemplated in the assessment of material adverse impact in paragraph 34. While APRA's intent seems clear that these tolerance levels should focus

+61 2 8005 1265
Level 8, 299 Elizabeth St.
Sydney, NSW 2000, Australia

info@protechtgroup.com
www.protechtgroup.com

on the customer, the tolerance level of the entity and the tolerance level of the customer may differ. We recommend this is made clearer in the standard and / or guidance.

Maximum extent of data loss

We anticipate challenges with regulated entities establishing tolerance levels for data loss in accordance with 37(a) without further guidance. We do not anticipate that APRA provide prescriptive requirements, however we note the following issues that may challenge entities in setting their tolerance levels:

- A single data source may support multiple critical operations
- The data required to perform any particular critical operation may come from several discrete data sources
- Different types of data – and different combinations of data - may have different impacts on customers depending on the nature of the critical operation.
- Whether 'data loss' should be measured in terms of volume (potentially broken down by data type), timeframes (such as Recovery Point Objectives), both, or some other criteria.

Interrelationship between maximum period and minimum service levels

We expect that minimum service levels are likely to be descriptive in nature, supported by metrics where appropriate. We also query whether entities need to articulate how quickly those minimum service levels will be active after the initial disruption. This may be best explained by an example.

We will assume a fictional payments process that normally processes within 30 seconds, and this critical operation has a maximum tolerance level of 2 days. It is disrupted and a BCP is activated with alternative arrangements. Payments can now be processed with a minimum service level of 2 hour processing time. However the BCP contingency takes 6 hours to fully activate. While the minimum service level might be set at 2 hours, alternative arrangements cannot be activated within that timeframe.

PROTECHT
Redefining Risk

+61 2 8005 1265
Level 8, 299 Elizabeth St.
Sydney, NSW 2000, Australia

info@protechtgroup.com
www.protechtgroup.com

We assume more generally that these minimum service levels may include metrics or descriptors such as:

- % of normal volume of transactions that can be processed during disruption
- Process cycle times during disruption
- Contact centre wait times during disruption

Given the requirement to establish minimum service levels 'during disruption' in paragraph 37(c), a potential interpretation is that the critical operation should be restored in full – not to a functional but substandard level of service – prior to the maximum tolerance level established in paragraph 37(a). This may be a point of clarification in further guidance on whether entities can still be in some state of recovery beyond the tolerance level contemplated in paragraph 37(a).

PROTECHT
Redefining Risk

+61 2 8005 1265
Level 8, 299 Elizabeth St.
Sydney, NSW 2000, Australia

info@protechtgroup.com
www.protechtgroup.com

RESPONSE TO SPECIFIC PARAGRAPHS OF THE STANDARD

We outline here some specific paragraphs of the draft standard, and our questions or comments. In many cases we do not disagree with the principles or clauses of the draft standard, but may identify areas to be further considered or articulated in APRA's guidance planned for consultation in early 2023.

12. An APRA-regulated entity must identify, assess and manage operational risks that may result from inadequate or failed internal processes or systems, the actions or inactions of people or external drivers and events. Operational risk is inherent in all products, activities, processes and systems.

We note that the commonly accepted definition of risk is 'the effect of uncertainty on objectives' as outlined in the ISO 31000 standard on risk management, and therefore risks cannot be managed without first understanding objectives (in this case the regulated entities objectives). We appreciate that APRA's focus, as the regulator, is on reducing consumer harm and protecting the integrity of financial system. Risk is inherent in all products, activities, processes and systems to the extent they support achievement of business objectives.

18.Where APRA considers an APRA-regulated entity's operational risk management has material weaknesses, APRA may:

(a) require an independent review of the entity's operational risk management;

(b) require the entity to develop a remediation program;

(c) require the entity to hold additional capital, as relevant;

(d) impose conditions on the entity's licence; and

(e) take other actions required in the supervision of this Prudential Standard.

We note that there is no definition of material weakness in the standard. We anticipate APRA will provide some additional guidance on what may constitute a material weakness.

21(b) The Board must approve the BCP and tolerance levels for disruptions to critical operations, review the results of testing and oversee the execution of any findings.

PROTECHT
Redefining Risk

+61 2 8005 1265
Level 8, 299 Elizabeth St.
Sydney, NSW 2000, Australia

info@protechtgroup.com
www.protechtgroup.com

We propose rewording '*...execution of any findings*'. This is based on the assumption that a 'finding' is what is observed, such as a control weakness or steps in a tested BCP that do not achieve the desired outcome. A finding cannot be executed; agreed action in response to a finding can be executed.

21(c) The Board must approve the service provider management policy, and review risk and performance reporting on material service provider arrangements.

We note that paragraphs 21(a) and 21(b) are more explicit that the Board must ensure weaknesses are addressed. This paragraph only states that the Board must review risk and performance reporting but does not require the Board to ensure action is taken. It may be implied that this paragraph on material service provider arrangements forms part of the entities operational risk profile in paragraph 21(a), however if this is the intent it could be made more explicit.

23.An APRA-regulated entity must manage its full range of operational risks, including but not limited to legal risk, regulatory risk, compliance risk, conduct risk, technology risk, data risk, reputational risk and change management risk. Senior management are responsible for operational risk management across the end-to-end process for all business operations.

We note the following definition in *APS 001 Definitions*:

> ***Operational risk*** *means the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk but excludes strategic and reputational risks.*

This definition states that it excludes reputational risk, however reputational risk is included in paragraph 23 of the draft standard. Protecht's view is that reputation is not a risk, but is an impact or consequence that may arise from risks of any type.

26(b) An APRA-regulated entity must maintain a comprehensive assessment of its operational risk profile. As part of this, an APRA-regulated entity must identify and document the processes and resources needed to deliver critical operations, including people, technology, information, facilities

+61 2 8005 1265
Level 8, 299 Elizabeth St.
Sydney, NSW 2000, Australia

info@protechtgroup.com
www.protechtgroup.com

and service providers, the interdependencies across them, and the associated risks, obligations, key data and controls.

Protecht welcomes the requirements of this paragraph. In relation to *"…**associated** risks, obligations, key data and controls*", it is not clear whether APRA requires them to be associated to one or many of the preceding items. While we anticipate APRA intends for this paragraph to be up to regulated entities to interpret, if APRA has a more specific expectation on how those associations are to be demonstrated, we propose making them clear.

40. An APRA-regulated entity must maintain the capabilities required to execute the BCP, including access to people, resources and technology. An APRA-regulated entity must monitor compliance with its tolerance levels and report any failure to meet tolerance levels, together with a remediation plan, to the Board.

In relation to *"…must monitor compliance with its tolerance levels…",* the implication is that it only applies when disruption occurs. i.e. You can only be non-compliant with tolerance levels contemplated in paragraph 37 if they have been exceeded. If APRA intends for this to have application outside of disruptive events, we recommend this is made clearer. In contrast, the first sentence of clause 40 (maintain capabilities) appears to be an 'always on' obligation.

42. An APRA-regulated entity must have a systematic testing program for its BCP that covers all critical operations and includes an annual business continuity exercise. The program must test the effectiveness of the entity's BCP and its ability to meet tolerance levels in a range of severe but plausible scenarios.

Protecht question the practicality of an annual business continuity exercise. We anticipate that to achieve operational resilience outcomes, entities must test the effectiveness of their business continuity arrangements, and the robustness of their critical resources, on an ongoing review and testing cycle.

PROTECHT
Redefining Risk

+61 2 8005 1265
Level 8, 299 Elizabeth St.
Sydney, NSW 2000, Australia

info@protechtgroup.com
www.protechtgroup.com

44. An APRA-regulated entity must review and update, as necessary, its BCP on an annual basis to reflect any changes in legal or organisational structure, business mix, strategy or risk profile or for shortcomings identified as a result of the review and testing of the BCP.

We agree that an annual review to ensure accuracy of the BCP is appropriate. However, we suggest that the BCP should also be updated at the time any of the contemplated changes are made. This will avoid a BCP that may be ineffective if it is required to be activated between the time a significant business change is made and an annual review.

47(d).The [service provider management] policy must include the entity's approach to managing the risks associated with any fourth parties that material service providers rely on.

While this requirement is to include the entities approach to managing fourth party risk in the policy, the standard does not set any minimum expectations. For example, it could be argued that a single policy statement of 'we ask our material service providers to list the providers they rely on' would comply with this paragraph without any other activity. If APRA has any minimum expectations, these should be articulated.

Our interpretation is that, as worded, this only applies to fourth parties. i.e. It does not require a regulated entity to consider suppliers further in their supply chain. If APRA intends for entities to consider their complete supply chain (i.e. nth party) this should be made clearer. However we also anticipate extending beyond fourth parties creates significant challenges for regulated entities to effectively manage or comply with.

53.For all material service provider arrangements, an APRA-regulated entity must maintain a formal legally binding agreement. The formal agreement must, at a minimum:

(a) specify the services covered by the agreement and associated service levels;

(b) set out the rights, responsibilities and expectations of each party to the agreement, including in relation to the ownership of assets, ownership and control of data, dispute resolution, audit access, liability and indemnity;

(c) include provisions to ensure the ability of the entity to meet its legal and compliance obligations;

+61 2 8005 1265
Level 8, 299 Elizabeth St.
Sydney, NSW 2000, Australia

info@protechtgroup.com
www.protechtgroup.com

(d) require notification by the service provider of its use of other material service providers, through sub-contracting or other arrangements;

(e) require the liability for any failure on the part of any sub-contractor to be the responsibility of the service provider;

(f) include a force majeure provision indicating those parts of the contract that would continue in the case of a force majeure event; and

(g) termination provisions including, but not limited to, the right to terminate both the arrangement in its entirety or parts of the arrangement. For an RSE licensee, termination provisions must include the ability for the RSE licensee to terminate the arrangement where to continue the arrangement would be inconsistent with the RSE licensee's duty to act in the best financial interests of beneficiaries (refer to section 52(2)(c) of the SIS Act).

54.The formal agreement must also include provisions that:

(a) allow APRA access to documentation, data and any other information related to the provision of the service;

(b) allow APRA the right to conduct an on-site visit to the service provider; and

(c) ensure the service provider agrees not to impede APRA in fulfilling its duties as prudential regulator.

Paragraphs 53 and 54 place requirements on the regulated entities that may be difficult for some regulated entities to manage. As these are mandatory requirements for the entity, service providers have the power on whether they accept these conditions or not – or price their services and contracts to compensate. We also question what bargaining power smaller entities will have to enforce these clauses, particularly for renewal of existing contracts that fall under these paragraphs.

APRA may need to consider working with industry to ensure that meeting these requirements are available to any regulated ADI that contracts with critical technology/service providers. This will be particularly important given the concentration risk some of those critical technology/service providers represent.

+61 2 8005 1265
Level 8, 299 Elizabeth St.
Sydney, NSW 2000, Australia

info@protechtgroup.com
www.protechtgroup.com

57.An APRA-regulated entity must monitor and report to senior management on material service provider arrangements commensurate with the nature and usage of the service. This monitoring must include a regular assessment of:

(a) performance under the service agreement with reference to agreed service levels;

(b) the effectiveness of controls to manage the risks associated with the use of the service provider; and

(c) compliance of both parties with the service provider agreement.

We anticipate further guidance may be provided on the frequency of a 'regular assessment'.

CLOSING COMMENTS

We welcome the simplification of the standards by APRA. We agree with the approach that operational resilience is an outcome from taking an integrated approach to risk management.

We thank APRA for engaging the community in its consultation process. We look forward to further developments as the standard evolves and the opportunity to further contribute.

Kind regards,

[redacted]
Research & Content Lead
On behalf of Protecht Group

Endorsed by:
[redacted] – **Chief Research & Content Officer**
[redacted] – **Chief Executive Officer**