DELL Technologies

October 21, 2022

General Manager, Policy
Australian Prudential Regulation Authority

Submitted via email: PolicyDevelopment@apra.gov.au

**Re: Consultation on Draft Prudential Standard CPS 230 Operational Risk Management**

Dell Technologies **("Dell")** is grateful for the opportunity to provide comments to the Australian Prudential Regulation Authority's **("APRA")** public consultation on the Discussion Paper "Strengthening operational risk management", and on the draft Prudential Standard CPS230 Operational Risk Management **("Draft CPS 230").** We would be pleased to discuss our submission in greater detail with APRA as it moves to implement a cross-industry prudential standard for the management of operational risk as proposed in the draft standard.

If there is further information or clarification that we can provide to you in respect of this submission, please do not hesitate to contact me at [redacted]

Sincerely,

[redacted]

[redacted]
Consultant, APJ Global Alliances
Dell Technologies

**Part 1: Dell Technologies Response to the Discussion Paper and Draft CPS 230**

Subject to the specific comments and recommendations contained in this submission, Dell is broadly supportive of APRA's decision to consolidate several existing standards (CPS 231, CPS 232, SPS 231, SPS 232 and HPS 231) as detailed on page 5 of the Discussion Paper into a single, coherent Operational Risk Management Standard (CPS 230) that will be applicable to all regulated entities. Dell is also supportive of the overall thrust of the paper with regards to the strengthening of overall operation risk management, business continuity practices, and the management of risks associated with the use 3rd party service providers.

Dell has reviewed the Draft CPS 230 and in general we believe that it sets an appropriate standard for the management of operation risk by regulated entities. However we have identified several areas that we believe would benefit from further clarification and/or extension by APRA, given the changes in the technology platforms used by regulated entities, and the impacts that these changes have for the management of risk both within an entity and systemically.

## Part 2: Dell Technologies comments on draft standard CPS 230

*2.1 Development and maintenance of business continuity plans (Paragraph 15e)*

Dell's view is that an entity's business continuity planning must be sufficiently comprehensive and integrated so as to facilitate the production of a single business point of consistency across the entity's entire data landscape. Failure to achieve a single business point of consistency will result in the need for extended recovery times following a disruption as a result of the need to validate that all of the entity's data is appropriately synchronized, so as to guarantee true data integrity prior to the resumption of production processing.

Dell's rationale behind this recommendation is that the majority of APRA-regulated entities are large organizations and make use of what are commonly called federated application environments as part of delivering critical business functions. The use of potentially multiple business continuity plans that may be constructed based on the lines of business within the entity, specific applications or application groups, or based on where a particular process runs (eg. inhouse as compared to running at a service provider, or across any combination of the entity's inhouse IT environments and service providers) creates complexity and potentially complicates the production of a single business point of consistency, and hence likely increases the time required by the entity to recover from a disruption. Regulated entities need to be cognizant of the inter-relationships between all of their business processes, whether facilitated using inhouse environments or via external service providers, and their BCP(s) need to be thoroughly reflective of these inter-relationships.

*2.2 Monitoring of IT infrastructure by regulated entities (Paragraph 24)*

Dell's view is that it is not sufficient for an APRA-regulated entity to simply "..monitor the age and health of its IT infrastructure…", but rather that it must go further and additionally monitor the vendor support status of said IT infrastructure, as well as being accountable for the monitoring of the vendor support status and health of IT infrastructure used by 3rd party service providers who are providing services to the APRA-regulated entity.

The rationale behind Dell's recommendation to enhance the standard in this area is fairly simple. It is conceivable that although a component of an entity's IT infrastructure, either directly owned or provided by a service provider, may be relatively young in terms of age, if it or the software/firmware running on it is no longer supported by the vendor of the component an operational risk exposure is created that may lead to elongated or worse still unsuccessful remediation of component failure, or an increased potential for cyber security to be compromised. Ensuring that the hardware and associated code in use are fully supported by their respective vendors, and ideally running at target code levels or close to them, simply makes sense from a risk management perspective.

2.3 *Identification and documentation of interdependencies across processes and resources needed to deliver critical operations (Paragraph 26b)*

Dell's view is that in regulated entity IT environments that are increasingly federated, and that are built on a complex combination of inhouse and external service provider based operating environments, the understanding of the interdependencies and relationships between all sections of the entity's IT environment is essential. Paragraph 26 of the draft standard attempts to appropriately articulate what a regulated entity needs to do. There is however a potentially hidden set of interdependencies and relationships that Paragraph 26 of the draft standard does not cover, and that is the dependencies and relationships that exist within the operating environment in any service provider, and also that arise as a result of competing tenant workloads within a service provider. While such service provider related effects are typically dealt with under the terms of the service level agreement struck between the regulated entity and the service provider, it is probably outside the capability of an APRA-regulated entity to fully understand what all these additional service provider centric interdependencies and relationships are.

2.4 *Notification window for operational risk incidents (Paragraph 32)*

Dell's view is that it is notification of APRA "not later than 72 hours after becoming aware of an operational risk incident" is probably a little generous, given the potential contagion such an incident at a large regulated entity could have on the broader Australian financial environment. It is recommended that consideration be given to tightening this notification requirement.

2.5 *Business Continuity Plans (Paragraph 33c and footnote 11)*

See comments in section 2.1 above.

2.6 *Identification and management of risks affecting a service provider's ability to provide service (Paragraphs 55a & c)*

Dell does not believe that it is possible for an APRA-regulated entity to "identify and manage any risks that could affect the ability of the service provider to provide the service on an on-going basis", as in order to do so the regulated entity would need to have complete visibility into the service provider's environment and operations, and into the interactions of the competing tenant workloads that run within the service provider's environment. Dell's view is that consideration should be given to rewording this section in a way that recognizes the limitations that a regulated entity has in managing risk within a service provider.

Similarly, the ability of an APRA-regulated entity to "continue to execute its BCP" may be compromised by an issue within a material service provider that is beyond the scope of the regulated entity's ability to manage risk within the service provider's environment. Again it is Dell's view that consideration should be given to rewording this section so as to recognize the limitations that a regulated entity may have in this area.

It should be noted that neither of the comments above seek to diminish the responsibility that a service provider has to a regulated entity to meeting any agreed service level. To this end, it is suggested that APRA give consideration to defining what sorts of events should be excluded from being considered a force majeure event.

**Part 3: Additional issues relating to Operational Risk not covered in the Discussion Paper or Draft CPS 230**

Dell recommends that APRA give consideration to some additional issues that are strongly correlated with operational risk as part of its development of the new CPS 230 standard. Specifically, Dell believes that consideration should be given to addressing questions such as:

- What does APRA view as an acceptable service level for a regulated entity to acknowledge/process transactions that are meant to be handled in real time?
  - Under what circumstances would APRA accept a degradation to this service level, and by what amount?
- What does APRA view as an acceptable level of secondary or tertiary site data currency in disaster situations?
  - Putting this another way, how much data loss would APRA consider to be acceptable should a regulated entity lose its primary processing environment?
- What sorts of systemically induced operational risks does APRA believe regulated entities should be cognizant of and prepared to mitigate?