21 October 2022

Australian Prudential Regulation Authority
Level 12 , 1 Martin Place
Sydney NSW 2000
Email: PolicyDevelopment@apra.gov.au

Dear Sir/Madam

Re: Australian Prudential Regulation Authority (ARPA)'s Consultation on New Prudential Standard CPS 230 Operational Risk Management (CPS 230)

Salesforce is pleased to provide this submission to the APRA's draft Prudential Standard CPS 230 on Operational Risk Management.

About Salesforce

Salesforce is the #1 CRM, and an enterprise software company. Salesforce is a cloud computing company covering customer relationship management and other business-focused software to businesses, governments, and other organisations around the world. Salesforce is used by over 150,000 customers globally. In 1999, Salesforce pioneered the 1-1-1 Model which dedicates 1% of Salesforce's equity, 1% of Salesforce's product, and 1% of Salesforce employees' time back to communities around the world. Among Salesforce customers are financial service providers and institutions.

Our comments and recommendations are appended below.

Scope of Material Service Providers

Article 49 of the draft consultation provides a broad scope of the definition of "material service providers". Beyond third parties and related parties deemed material, the draft mentions that material service providers include those that provide risk management, core technology services, internal audit, credit assessment, funding and liquidity management, mortgage brokerage, underwriting, claims management, insurance brokerage, reinsurance, fund administration, custodial services, investment management and arrangements with promoters, financial planners and those that manage information assets classified as critical or sensitive under CPS 234. APRA may also classify a service provider, or type of service provider, as material.

Salesforce understands the need to reflect the increased dependency on third parties to provide

material operations. However, "core technology services", may be interpreted as overly broad. A technology service provider may provide a range of services to an APRA-regulated entity.

Recommendation #1: We encourage APRA to better define the scope of requirements and replace the term "core technology services" with a definition specifically limiting to critical services deemed material for enhanced clarity.

Geographic location

Article 52 refers to APRA-regulated entities which might not be best placed to evaluate "risks associated with geographic location" and whether the provider is "systematically important in Australia".

Requiring risk assessments based on the service provider's "geographic location" also restrict the number of products available for use by APRA-regulated entities, which may result in unintential consequences. The associated risk of the service should not be based on geographic location, but the security and privacy safeguards in place for that service.

Recommendation #2: That the reference to geographic location be removed.

Article 54 includes some of the mandatory contractual provisions between an APRA-regulated entity and its service providers, some of which include:

- allow APRA access to documentation, data and any other information related to the provision of the service;
- allow APRA the right to conduct an on-site visit to the service provider; and
- ensure the service provider agrees not to impede APRA in fulfilling its duties as prudential regulator

In some instances, these draft provisions may go beyond current existing contractual arrangements between ARPA-regulated entities and third-party providers, and could raise privacy and security concerns, and impact business confidentiality. Contractual arrangements between APRA-regulated entities and their service providers would typically include provisions that allow the former the ability to audit and inspect documentation and information related to the provision of those services.

APRA-regulated entities may contact Salesforce to request an on-site audit of Salesforce's processing activities under specific circumstances.

Furthermore, third-party service providers may also be contractually prohibited from accessing data on its services unless explicitly directed by its customers, a prohibition designed to increase security and privacy protections afforded to that data. In this regard, the requirement in Article 54(a) could be read

to allow APRA direct access to specific data which might inadvertently lead third-party service providers to be in breach of their contractual obligations to their APRA-regulated customers.

The establishment of the appropriate transition and termination arrangements in a contractual outsourcing agreement should be a joint responsibility between the APRA-regulated entity and service provider. At Salesforce, we have a holistic trust and compliance documentation, known as the Security, Privacy, and Architecture ("SPARC") which contains service specific information about the return and deletion of customer data.

Recommendation #3: APRA provide greater clarity on Article 54(a) and Article 53 draft provisions, and outline contractual agreements to be made between ARPA-regulated entities and third-party service providers instead of detailing minimum requirements, as some of these requirements may go beyond the existing contractual obligations with APRA-regulated entities.

Operational Risk Management

Article 23 requires APRA-regulated entities to 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.

In managing technology risks, an APRA-regulated entity is also required to monitor the age and health of its IT infrastructure and meet the requirements for information security in Prudential Standard CPS 234 Information Security (CPS 234).

At Salesforce, we have implemented technical and administrative security measures to help protect our services and customer data. Technical security measures include protections against system vulnerabilities, separation of customer data, network security, encryption of data in transmission, and options for encryption of data at rest. Administrative security measures include limiting access, comprehensive security policies on handling customer data, and security training and awareness programs.

Salesforce offers customers controllable features that permit them to configure the security settings of their Salesforce Services as they deem appropriate. The Salesforce Security Guide describes these features in detail. Further information on Salesforce security measures can be found on the Help & Training Portal or on the Salesforce.com website, including: Salesforce Security Guide, detailing customer controllable security features of Salesforce Services (including encryption); SPARC and sub-processor documentation; Force.com Multitenant Architecture paper; and Shield Platform Encryption Architecture paper.

Cyber Risk Incident Reporting

Article 32 requires service providers to report cyber incidents to their customer APRA-regulated entity no later than 72 hours, after determining that the incident is likely to have a material financial impact or a material impact on the ability of the entity to maintain its critical operations.

The cyber-incident reporting timeline of 72 hours is aligned with international best practices such as the EU's General Data Protection Regulation. The Salesforce Trust portal provides customers with access to valuable, real-time information regarding the current status of services. This includes service availability and performance, response times, security advisories, and security certifications, among others. Salesforce also provides support in the form of materials, resources and consultation.

Thank you for the opportunity to provide comments. Should you require further information please contact me at [redacted].

Yours sincerely

[redacted]
Vice President, Government Affairs & Public Policy, APAC