Cloudflare's Commentary on Contractual Requirements in APRA's CPS 230

Cloudflare has prepared this document to assist customers supervised by the Australian Prudential Regulation Authority ("**APRA**") to understand how Cloudflare's Enterprise Subscription Terms of Service ("**Agreement**") meet the contractual requirements set out in paragraphs 54 to 57 (service provider agreements) of the Prudential Standard CPS 230 - Operational Risk Management ("**CPS 230**") in the context of Cloudflare services including the incorporation of the Cloudflare Regulatory Exhibit into the Agreement.

No.	CPS 230 Provision	Cloudflare Commentary
1.	54. For all material arrangements, an APRA-regulated entity must maintain a formal legally binding agreement (formal agreement). The formal agreement must, at a minimum:	The Agreement which is either executed by the customer and Cloudflare, or passed through to the end customer by a reseller, governs the customer's subscription to Cloudflare services.
2.	54(a). specify the services covered by the agreement and associated service levels;	The subscription to the Cloudflare services are governed by the Agreement (section 2.1 of the Agreement). The Cloudflare services are described on Cloudflare's website. Service levels relating to Cloudflare services are set out in the Cloudflare Enterprise Customer Support and Service Level Agreement.
3.	54(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;	The rights and responsibilities of the parties are set out in the Agreement. Ownership of assets: Except for the limited rights expressly stated in the Agreement, no rights, implied or otherwise, are granted to the customer's intellectual property. Ownership and control of data: Customer owns all Intellectual Property Rights in Customer Data (Section 6.1 of the Agreement). The Agreement grants limited rights for Cloudflare to use the information customer provides upon subscribing to the Cloudflare service, audit logs, and customer account settings ("**Customer**

No.	CPS 230 Provision	Cloudflare Commentary
		Account Information") for business purposes related to the Agreement, and to the extent necessary to meet Cloudflare's legal compliance obligations (including, for audit and anti-fraud purposes) (section 6.2 of the Agreement). The ordinary operation of the Cloudflare services requires Customer Data to pass through Cloudflare's network. Cloudflare has a limited right to use the Customer Data solely as permitted under the Agreement and as required to provide Cloudflare services (section 5.3 of the Agreement). To the extent that Cloudflare processes Customer Data on behalf of the customer that includes Personal Data, Cloudflare will handle such Personal Data in compliance with the Data Processing Addendum ("**DPA**"). Dispute resolution: Dispute resolution is set out in section 12.1 of the Agreement. Audit access: Cloudflare proactively takes on the expense and effort to undergo accredited third party audits to assure our customers of effective security controls. At least annually, Cloudflare engages with an independent assessor to conduct a compliance assessment and provide a full attestation, review or report under (A) Service Organization Control (SOC 2 Type II) or (B) other similar industry recognized independent compliance assessment, including ISO 27001, PCI-DSS, and provide these reports and certifications to customer upon request (section 11 of Cloudflare's Information Security Exhibit ("**ISE**"). Reporting obligations are set out in both the DPA and the ISE. Additional audit rights are set out in the Regulatory Exhibit. Liability: Indirect liability is excluded and can be mutualised for customer on

No.	CPS 230 Provision	Cloudflare Commentary
		our papered Agreement. Direct damages are subject to a liability cap and can be mutualised for customer on our papered Agreement subject to certain exclusions including in relation to matters that cannot be excluded or limited under applicable Law and indemnification obligations (section 9 of the Agreement). Indemnity: Cloudflare provides third party intellectual property right indemnification (section 10.1 of the Agreement).
4.	54(c). include provisions to ensure the ability of the entity to meet its legal and compliance obligations;	Cloudflare warrants that in connection with its performance of the agreement, it will comply with all Laws including, but not limited to, laws related to data privacy, international communications and the transmission of technical or Personal Data as defined in the DPA (section 7.1 of the Agreement.
5.	54(d). require notification by the service provider of its use of other material service providers that it materially relies upon in providing the service to the APRA-regulated entity through sub-contracting or other arrangements;	Additional obligations relating to sub-contractors are set out in the Regulatory Exhibit. Cloudflare maintains a list of sub-processors on the Cloudflare Sub-Processors page. There is no express notification to customers of new and replacement sub-processors, but the names of new and replacement sub-processors will be added to the list at least thirty (30) days prior to the date on which those sub-processors commence processing of Personal Data. (section 4.4 of the DPA).
6.	54(e). require the liability for any failure on the part of any sub-contractor to be the responsibility of the service provider;	Cloudflare is liable to the customer for any breach by a sub-processor of any Relevant Terms (section 4.2 of the DPA). If the customer procures migration services from Cloudflare, whether directly or indirectly through a reseller, and where Cloudflare engages sub-contractor(s) to perform any of its obligations relating to the migration services, the Statement of Work will include additional terms and conditions that state that Cloudflare remains responsible for the performance of any sub-contractor.

No.	CPS 230 Provision	Cloudflare Commentary
7.	54(f). include a force majeure provision indicating those parts of the contract that would continue in the case of a force majeure event; and	Force majeure provisions are set out in Section 12.9 of the Agreement.
8.	54(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 subsection 52(2)(c) of the SIS Act).	Subscriptions can be terminated by providing a written notice of non-renewal at least two (2) months before the expiry of the then-current Order Form Term (section 11.2 of the Agreement). Subscriptions and the Agreement can be terminated for cause e.g. uncured material breach of the Agreement (section 11.3 of the Agreement). Additional termination rights due to APRA's orders are set out in the Regulatory Exhibit.
9.	55. The formal agreement must also include provisions that:	
10.	55(a). allow APRA access to documentation, data and any other information related to the provision of the service;	Additional rights for APRA to access documentation, data and any other information related to the provision of the Cloudflare services are set out in the Regulatory Exhibit.
11.	55(b). allow APRA the right to conduct an on-site visit to the service provider; and	Additional rights for APRA to conduct audits are set out in the Regulatory Exhibit.
12.	55(c). ensure the service provider agrees not to impede APRA in fulfilling its duties as prudential regulator.	Right for APRA to fulfill its duties as prudential regulator without impediment is incorporated in the Agreement pursuant to the Regulatory Exhibit.
13.	56. For each material arrangement an APRA-regulated entity must:	
14.	56(a). identify and manage risks that could affect the ability of the service provider to provide the service on an ongoing basis;	Penetration Testing: Cloudflare will perform routine network and application-level scans for vulnerabilities and will remediate them according to industry standards (e.g. PCI DSS) (section 8.1 of the ISE).

No.	CPS 230 Provision	Cloudflare Commentary
		At least once every year, Cloudflare will engage an independent third-party security firm to perform a network and web application penetration test. Upon request, Cloudflare will provide a summary of the results of the penetration tests (section 8.2 of the ISE). Cloudflare will apply security patches and system updates to Cloudflare-managed software and applications, appliances, and operating systems according to industry standards (e.g. PCI DSS) (section 8.3 of the ISE). <u>Performance standards, uptime and support response times:</u> The Cloudflare Service will serve Customer Content measurably faster than customer's websites would serve Customer Content without use of the Service (section 2.1 of the SLA). The Cloudflare Service will serve Customer Content globally 100% of the time (section 2.2 of the SLA). Cloudflare's initial response times for support are set out in section 5 of the SLA. <u>Risk management program:</u> Cloudflare has designed its risk management program based on industry best practices from NIST SP 800-39 and the ISO 27005 and 31000. The program includes processes for identifying risk through audits, risk assessments, vulnerabilities, incidents, and third party security reviews. Risks are assessed on a low, moderate, and high scale. Risk is calculated based on the probability they will occur, taking into account threat and vulnerability factors, and the impact to Cloudflare and its customers. The risk register is updated on an ongoing basis and reviewed at least quarterly by the GRC and Security Leadership Teams. Governance and reporting structures are in place to ensure the appropriate risk response is applied, risk acceptance is periodically reviewed, and that risk is reported to executive level committees.
15.	56(c). ensure it can execute its BCP if needed; and	Cloudflare will maintain a documented and operational business

No.	CPS 230 Provision	Cloudflare Commentary
		continuity and disaster recovery ("**BC&DR**") program, exercise and update them at least annually, and provide a summary of the exercise upon request (section 9 of the ISE). BC&DR processes primarily affect the core and are frequently updated. Edge services that protect customer sites and deliver CDN are highly redundant and have a 100% uptime SLA. Our BC&DR program is tested in our SOC 2 audit. A summary of the most recent DR exercise is available upon request.
16.	56(d). ensure it can conduct an orderly exit from the arrangement if needed.	Customers have continuous access during the life of the engagement to manage their own use of the services, including automatic export of their data from Cloudflare. Cloudflare will use reasonable efforts to allow Customer to have access to Customer Logs for up to seventy-two (72) hours following expiration or termination of customer's access to the Cloudflare Service (section 11.5 of the Agreement). Cloudflare does not have any formal or packaged disengagement or transition services, and we would need customer to define the type of activities that customer would like supported in order to scope or service any such request.
17.	57. APRA may require an APRA-regulated entity to review and make changes to a service provider arrangement where it identifies heightened prudential concerns.	Cloudflare is committed to working in good faith with customer to address any concerns arising from any change in APRA Prudential Standards to the extent applicable to Cloudflare.