APRA Prudential Standard CPS 231 Outsourcing

G Suite Mapping

This document is designed to help financial institutions regulated by the Australian Prudential Regulation Authority ("**APRA**") to consider Prudential Standard CPS 231 Outsourcing ("**CPS 231**") in the context of G Suite and the Google Cloud Financial Services contract.

We focus on paragraphs 28 to 30 (the outsourcing agreement) and paragraphs 34 and 36 (APRA access to services providers) of CPS 231. For each paragraph, we provide commentary to help you understand how you can address the requirements using the Google Cloud services and the Google Cloud Financial Services Contract.

#	APRA CPS 231	Google Cloud Commentary	Google Cloud Financial Services Contract Reference
1.	**The outsourcing agreement**		
2.	28. Each outsourcing arrangement must be contained in a documented legally binding agreement, except where otherwise provided in this Prudential Standard. The agreement must be signed by all parties to it before the outsourcing arrangement commences	The arrangement for the G Suite services is documented in the Google Cloud Financial Services Contract. This is executed by both parties.	N/A
3.	29. At a minimum, the agreement (including arrangements with related bodies corporate) must address the following matters:		
4.	(a) the scope of the arrangement and services to be supplied;	The G Suite services are described on our services summary page. You decide which services to use, how to use them and for what purpose. Therefore, you decide the scope of the arrangement.	Definitions
5.	(b) commencement and end dates;	Refer to your Google Cloud Financial Services Contract.	Term and Termination
6.	(c) review provisions;	Evaluation of controls Google recognizes that you expect independent verification of our security, privacy and compliance controls. Google undergoes several independent third-party audits on a regular basis to provide this assurance. Google commits to comply with the following key international standards during the term of our contract with you: • ISO/IEC 27001:2013 (Information Security Management Systems) • ISO/IEC 27017:2015 (Cloud Security) • ISO/IEC 27018:2014 (Cloud Privacy) • SOC 1 • SOC 2 • SOC 3 You can review Google's current certifications and audit reports at any time.	Certifications and Audit Reports

APRA Prudential Standard CPS 231 Outsourcing

G Suite Mapping

		• Google's **ISO certifications** are available on our Compliance Resource Center. • Google's **SOC reports** and **PCI Attestation of Compliance (AOC)** are available to customers under NDA and can be requested from your Google Cloud account representative.. Google is audited at least once a year for each audited framework. The audit scope covers in scope Services, infrastructure systems, policies and procedures, common processes and personnel. Google engages certified and independent third party auditors for each audited framework. Refer to the relevant certification or audit report for information on the certifying or auditing party. Ongoing Oversight Google recognizes that to effectively manage your use of the Services you need sufficient information about the Services on a regular basis. We provide a number of notification mechanisms to assist you to effectively oversee the Services on an ongoing basis. Refer to rows 10, 11 and 17. In addition, as your use of the Services or the regulatory environment evolves, Google appreciates that you will need to have confidence that the Google Cloud Financial Services Contract continues to support your compliance requirements. We are committed to working with you throughout our relationship to address the impact of changes in law or regulation. If, however, for whatever reason, you wish to stop using our Services, you can do so at any time.	Enabling Customer Compliance; Termination for Convenience
7.	(d) pricing and fee structure;	Refer to your Google Cloud Financial Services Contract. Prices and fee information are also publicly available on our Pricing page.	Payment Terms
8.	(e) service levels and performance requirements;	The SLAs are available on our G Suite Service Level Agreement page.	Services
9.	(f) the form in which data is to be kept and clear provisions identifying ownership and control of data;	Form Google encrypts customer data stored at rest by default, with no additional action required from you. More information about encryption is available on our Google Cloud Help page. You can further define the security of your data and applications. Refer to row 13. Ownership	Intellectual Property

APRA Prudential Standard CPS 231 Outsourcing

G Suite Mapping

		You retain all intellectual property rights in your data. Control You can provide Google instructions about your data and Google will comply with those instructions.	Google's Compliance with Instructions (Data Processing Amendment)
10.	(g) reporting requirements, including content and frequency of reporting;	Google will make information about developments that materially impact Google's ability to perform the Services in accordance with the SLAs available to you. More information is available on our G Suite Status Dashboard. In addition, Google will notify you of data incidents promptly and without undue delay. More information on Google's data incident response process is available in our Data incident response whitepaper.	Significant Developments Data Incidents (Data Processing Amendment)
11.	(h) audit and monitoring procedures;	Audit Google grants audit, access and information rights to institutions and their appointees. This includes access to both documentation and information and the right to conduct onsite visits. Nothing in our contract is intended to impede or inhibit an institution's ability to audit our services effectively. In particular, although we will make a lot of information and tools available to help institutions review our Services, our contract does not contain caveats or pre-defined steps before institutions can approach Google to exercise their audit, access and information rights. In other words, there is no hierarchy amongst the options for assessing our Services. Monitoring You can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services. For example: • The **Status Dashboard** provides status information on the Services. • **Admin Console Reports** allow you to examine potential security risks, measure user collaboration, track who signs in and when, analyze administrator activity, and much more.	Customer Information, Audit and Access Ongoing Performance Monitoring

APRA Prudential Standard CPS 231 Outsourcing

G Suite Mapping

		• **Access Transparency** is a feature that enables you to review logs of actions taken by Google personnel regarding your data. Log entries include: the affected resource, the time of action, the reason for the action (e.g. the case number associated with the support request); and data about who is acting on data (e.g. the Google personnel's location).	
12.	(i) business continuity management;	Google will implement a business continuity plan for the Services, review and test it at least annually and ensure it remains current with industry standards. More information on the reliability of the Services is available on our Google Cloud Help page.	Business Continuity and Disaster Recovery
13.	(j) confidentiality, privacy and security of information;	This is addressed in the Data Processing Amendment where Google makes commitments to protect your data, including regarding security, deletion, access and transfer. The confidentiality, privacy and security of a cloud service consists of two key elements: Google's infrastructure Google manages the security of our infrastructure. This is the security of the hardware, software, networking and facilities that support the Services. Given the one-to-many nature of our service, Google provides the same robust security for all our customers. This is described in the Data Processing Amendment. Google provides detailed information to customers about our security practices so that customers can understand them and consider them as part of their own risk analysis. More information is available at: • Our infrastructure security page • Our security whitepaper • Our cloud-native security whitepaper • Our infrastructure security design overview page • Our security resources page In addition, you can review Google's SOC 2 report. Refer to row 6. Your data and applications in the cloud You define the security of your data and applications in the cloud. This refers to the security measures that you choose to implement and operate when you use the	Confidentiality Data Security; Security Measures (Data Processing Amendment)

		Services. (a) Security by default Although we want to offer you as much choice as possible when it comes to your data, the security of your data is of paramount importance to Google and we take the following proactive steps to assist you: • **Encryption at rest.** Google encrypts certain data while it is stored at rest on a disk (including solid-state drives) or backup media. Even if an attacker or someone with physical access obtains the storage equipment containing your data, they won't be able to read it because they don't have the necessary encryption keys. • **Encryption in transit.** Google encrypts all data while it is "in transit"--traveling over the Internet and across the Google network between data centers. Should an attacker intercept such transmissions, they will only be able to capture encrypted data. at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. See our G Suite encryption whitepaper for more information. (b) Security products In addition to the other tools and practices available to you outside Google, you can choose to use tools provided by Google to enhance and monitor the security of your data. Information on Google's security products is available on our Cloud Security Products page. (c) Security resources Google also publishes guidance on: • Security best practices • Security use cases	
14.	(k) default arrangements and termination provisions;	Termination	Term and Termination

APRA Prudential Standard CPS 231 Outsourcing

G Suite Mapping

		In addition to being able to terminate for material breach, institutions can elect to terminate our contract for convenience, including if necessary to comply with law or if directed by the competent authority. Transition Term Google recognizes that institutions need to be able to exit our Services without undue disruption to their business, without limiting their compliance with regulatory requirements and without any detriment to the continuity and quality of their service to their own clients. To help institutions achieve this, upon request, Google will continue to provide the Services for 12 months beyond the expiry or termination of the contract. Data export Google will enable you to access and export your data throughout the duration of our contract and the transition term. More information is available on our Google Account help page. In addition, **Data Export** is a feature that makes it easy to export and download a copy of your data securely from our Services.	Transition Term Data Export (Data Processing Amendment)
15.	(l) dispute resolution arrangements;	Refer to your Google Cloud Financial Services Contract.	Governing Law
16.	(m) liability and indemnity;	Refer to your Google Cloud Financial Services Contract.	Liability; Indemnification
17.	(n) sub-contracting;	Google recognizes that institutions need to consider the risks associated with sub-contracting. We also want to provide you and all our customers with the most reliable, robust and resilient service that we can. In some cases there may be clear benefits to working with other trusted organizations e.g. to provide 24/7 support. To enable institutions to retain oversight of any sub-outsourcing and provide choices about the services institutions use, Google will: ● provide information about our subcontractors; ● provide advance notice of changes to our subcontractors; and ● give institutions the ability to terminate if they have concerns about a new subcontractor.	Google Subcontractors

APRA Prudential Standard CPS 231 Outsourcing

G Suite Mapping

		Google will oversee the performance of all subcontracted obligations and ensure our subcontractors comply with our contract with you.	
18.	(o) insurance; and	Google will maintain insurance cover against a number of identified risks.	Insurance
19.	(p) to the extent applicable, offshoring arrangements (including through subcontracting).	Locations To provide you with a fast, reliable, robust and resilient service, Google may store and process your data where Google or its subprocessors maintain facilities. • Information about the location of Google's facilities is available on our Data Center Locations page. • Information about the location of Google's subprocessors' facilities is available on our subprocessor page. Google provides the same contractual commitments and technical and organizational measures for your data regardless of the country / region where it is located. In particular: • The same robust security measures apply to all Google facilities, regardless of country / region. • Google makes the same commitments about all its subprocessors, regardless of country / region. Options Google provides you with choices about where to store your data. Once you choose where to store your data, Google will not store it outside your chosen region(s). More information is available on our Data Regions page.	Data Regions (Service Specific Terms)
20.	30. An APRA-regulated institution that outsources a material business activity must ensure that its outsourcing agreement includes an indemnity to the effect that any sub-contracting by a third party service provider of the outsourced function will be the responsibility of the third party service provider, including liability for any failure on the part of the sub-contractor.	Google requires our subcontractors to meet the same high standards that we do. In particular, Google requires our subcontractors to comply with our contract with you and will remain liable to you for any subcontracted obligations.	Subcontracting; Google Subcontractors
21.	**APRA access to service providers**		
22.	34. An outsourcing agreement must include a clause that allows APRA access to documentation and information related to the outsourcing arrangement. In the normal course, APRA will seek to obtain whatever information it requires from the APRA-regulated institution; however, the outsourcing agreement must include the	Google grants audit, access and information rights to competent authorities and their appointees. This includes access to both documentation and information and the right to conduct onsite visits.	Regulator Information, Audit and Access

	right for APRA to conduct on-site visits to the service provider if APRA considers this necessary in its role as prudential supervisor. APRA expects service providers to cooperate with APRA's requests for information and assistance. If APRA intends to undertake an on-site visit to a service provider, it will normally inform the APRA-regulated institution of its intention to do so.	Nothing in our contract is intended to impede or inhibit the competent authority's ability to audit our services effectively. In particular, although we will make a lot of information and tools available to help competent authorities review our Services, our contract does not contain caveats or pre-defined steps before competent authorities can approach Google to exercise their audit, access and information rights. In other words, there is no hierarchy amongst the options for assessing our Services. Google will cooperate with competent authorities exercising their audit, access and information rights.	Enabling Customer Compliance
23.	36. An APRA-regulated institution must take all reasonable steps to ensure that a service provider will not disclose or advertise that APRA has conducted an onsite visit, except as necessary to coordinate with other institutions regulated by APRA that are existing clients of the service provider.	An onsite visit by your competent authority would be confidential as between you and Google.	Confidentiality