Australian Prudential Regulation Authority - Prudential Standard - CPS 230: Operational Risk Management

Google Cloud Mapping

This document is designed to help service providers supervised by the Australian Prudential Regulation Authority (“**regulated entity**”) to consider Prudential Standard CPS 230 - Operational Risk Management (“**framework**”) in the context of Google Cloud and the Google Cloud Financial Services Contract.

We focus on the following requirements of the framework: Service Provider Agreements paragraphs 53 to 57 . 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.

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
1	53. *Service provider agreements:* Before entering into or materially modifying a material arrangement, an APRA-regulated entity must:		
2	53 a. undertake appropriate due diligence, including an appropriate selection process and an assessment of the ability of the service provider to provide the service on an ongoing basis; and	Google recognizes that you need to conduct due diligence and perform a risk assessment before deciding to use our services. To assist you, we’ve provided the information below. In addition, Google collaborates with third-party risk management (TPRM) providers to support your cloud assessments. TPRM providers perform regular assessments of Google Cloud’s platform and services—they inspect hundreds of security, privacy, business continuity, and operational resiliency controls aligned with industry standards and regulations such as NIST SP 800-53, NIST CSF, ISO 27001, PCI-DSS, HIPAA, CMMC, SOC2, CSA STAR, and more. Based on their observations and assessments, TPRM providers develop independent audit reports that can help scale and accelerate your own risk assessment processes. For more information, refer to our Google Cloud risk assessment resources page. Google Cloud has been providing cloud services for over 10 years, assisting customers across the globe in the financial services, healthcare & life science, retail and public sectors to name a few. More information on Google Cloud’s capabilities is available on our Choosing Google Cloud page. Google Cloud has been named as a leader in several reports by third party industry analysts. You can read these on our Analyst Reports page. Information about our referenceable customers is available on our Google Cloud Customer page. In addition, our Financial Services Cloud Blog and Financial Services solutions page explains how financial services institutions can and are using Google Cloud to help drive business transformation to support data-driven innovation, customer expectations, and security & compliance. You can review information about Google’s historic performance of the services on our Google Cloud Service Health Dashboard.	N/A
3	53 b. assess the financial and non-financial risks from reliance on the service provider, including risks associated with geographic location or concentration of the service provider(s) or parties the service provider relies on in providing the service;	Location To provide you with a fast, reliable, robust and resilient service, Google may store and	

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		process your data where Google or its subprocessors maintain facilities. • Information about the location of Google's facilities and where individual Google Cloud services can be deployed is available on our Global Locations page. • Information about the location of Google's subprocessors' facilities is available on our Google Cloud subprocessors 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. 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) You can also choose to use tools provided by Google to enforce data location requirements. For more information, see our Data residency, operational transparency, and privacy for customers on Google Cloud Whitepaper. Concentration risk Google recognizes the importance of continuity for regulated entities and for this reason we are committed to data portability and open-source. Refer to our Engaging in a dialogue on customer controls and open cloud solutions blog post and our Open Cloud page for more information on how Google's approach to open source can help you address vendor lock-in and concentration risk. To manage concentration risk, you can choose to use Anthos to build, deploy and optimize your applications in both cloud and on-premises environments. Anthos provides a platform to develop, secure and manage applications across hybrid and multi-cloud environments. For more information, refer to the IDC Whitepaper on How A Multicloud Strategy Can Help Regulated Organizations Mitigate Risks In Cloud.	Data Transfers (Cloud Data Processing Addendum) Data Security; Subprocessors (Cloud Data Processing Addendum) Data Transfers (Cloud Data Processing Addendum) Data Export (Cloud Data Processing Addendum)

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		Subcontractors Google recognizes that regulated entities need to consider the risks associated with subcontracting. To enable regulated entities to retain oversight of any subcontracting and provide choices about the services regulated entities use, Google will: ● provide information about our subcontractors; ● provide advance notice of changes to our subcontractors; and ● give regulated entities the ability to terminate if they have concerns about a new subcontractor.	Google Subcontractors
4	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 use of the Services is governed by the Google Cloud Financial Services Contract.	N/A
5	54 a. specify the services covered by the agreement and associated service levels;	The Google Cloud services are described on our services summary page. The SLAs provide measurable performance standards for the services and are available on our Google Cloud Platform Service Level Agreements page.	Definitions Services
6	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 Google Cloud Financial Services Contract. Ownership You retain all intellectual property rights in your data, the data you derive from your data using our services and your applications, both during the term and after termination. Control You operate the services independently without action by Google personnel. You decide which services to use, how to use them and for what purpose. You also decide what data you provide to the services under your account and may access your data on the services at any time. Google commits to only access or use your data to provide the Services ordered by you and will not use it for any other Google products, services, or advertising. Regulated entities have the right to issue instructions to Google. To do this, regulated entities can use the following functionality of the Services:	Intellectual Property Protection of Customer Data Instructions

Australian Prudential Regulation Authority - Prudential Standard - CPS 230: Operational Risk Management

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		• Cloud Console: A web-based graphical user interface that customers can use to manage their Google Cloud resources. • gcloud Command Tool: A tool that provides the primary command-line interface to Google Cloud. A command-line interface is a user interface to a computer's operating system. • Google APIs: Application programming interfaces which provide access to Google Cloud. • Dispute resolution Refer to your Google Cloud Financial Services Contract. Audit Google recognizes that regulated entities and their supervisory authorities must be able to audit our services effectively. Google grants information, audit and access rights to regulated entities, supervisory authorities, and both their appointees. In addition, 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) • PCI DSS • SOC 1 • SOC 2 • SOC 3 You can review Google's current certifications and audit reports at any time. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources. Liability	Governing Law Customer Information, Audit and Access Regulator Information, Audit and Access Certifications and Audit Reports

Australian Prudential Regulation Authority - Prudential Standard - CPS 230: Operational Risk Management

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		Refer to your Google Cloud Financial Services Contract. Indemnity Google provides regulated entities with an indemnity for certain third party claims. Refer to your Google Cloud Financial Services Contract.	Liability Indemnification
7	54 c. include provisions to ensure the ability of the entity to meet its legal and compliance obligations;	Google recognizes that regulated entities require assistance from Google to enable them to ensure compliance with applicable laws and regulations. We are committed to working with regulated entities in good faith to provide this assistance.	Enabling Customer Compliance
8	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;	Google recognizes that regulated entities need to consider the risks associated with subcontracting. To enable regulated entities to retain oversight of any subcontracting and provide choices about the services regulated entities use, Google will: ● provide information about our subcontractors; ● provide advance notice of changes to our subcontractors; and ● give regulated entities the ability to terminate if they have concerns about a new subcontractor.	Google Subcontractors
9	54 e. require the liability for any failure on the part of any sub-contractor to be the responsibility of the service provider;	Google will remain liable to you for any subcontracted obligations.	Google Subcontractors
10	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	Refer to your Google Cloud Financial Services Contract.	Force Majeure
11	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).	Regulated entities can elect to terminate our contract for convenience with advance notice, including: ● if necessary to comply with law; and ● if directed by a supervisory authority.	Term and Termination
12	55 The formal agreement must also include provisions that:		
13	55 a. allow APRA access to documentation, data and any other information related to the provision of the service;	Google recognizes that regulated entities and their supervisory authorities must be able to audit our services effectively. Google grants information, audit and access rights to regulated entities, supervisory authorities, and both their appointees.	Regulator Information, Audit and Access

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		You may access your data on the services at any time. Regulated entities may provide their supervisory authority with access.	
14	55 b. allow APRA the right to conduct an on-site visit to the service provider; and	Refer to Row 13 for more information on information, audit and access rights. These include access to Google's premises used to provide the Services to conduct an on-site audit.	Regulator Information, Audit and Access
15	55 c. ensure the service provider agrees not to impede APRA in fulfilling its duties as prudential regulator.	Google will cooperate with supervisory authorities, resolution authorities and their appointees exercising their information, audit and access rights. Nothing in our contract is intended to limit or impede a regulated entity's or the supervisory authority's ability to audit our services effectively.	Enabling Customer Compliance
16	56 For each material arrangement an APRA-regulated entity must:		
17	56 a. identify and manage risks that could affect the ability of the service provider to provide the service on an ongoing basis;	Risk management Google recognizes that you need to plan and execute your migration carefully. Our Migration to Google Cloud guide helps you plan, design, and implement the process of migrating your workloads to Google Cloud to avoid and mitigate risk. In addition, our How to put your company on a path to successful cloud migration whitepaper provides guidance to help with the start of your digital transformation. The mechanisms used to secure and control cloud technologies can be substantially different to those used for on-premise technologies. Given that, it is important that your organization's control functions re-evaluate relevant key controls: even if the objectives behind existing controls are still valid, the specifics of the control, and the approach to managing it, will often need to evolve in order that the original control objective is still met in a cloud environment. In fact, using cloud native controls instead of relying on existing controls will often produce better outcomes because they are designed with cloud in mind. Refer to our Board of Directors Handbook for Cloud Risk Governance and Risk Governance of Digital Transformation in the Cloud whitepaper for more information, including about how control design and ownership evolves in the cloud. 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:	Ongoing Performance Monitoring

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		• The Service Health Dashboard provides status information on the Services. • Google Cloud Operations is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on Google Cloud, including availability and uptime of the services. • 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). Google proactively performs resilience testing, dependency identification, and mapping to find potential single points of failure, and then works proactively to correct any issues to minimize the impact of disruptions on customers. Services at Google are continuously monitored for their availability and graded against their SLO metrics. More information is available in our Infrastructure Design for Availability and Resilience whitepaper. 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 mechanisms to assist you to effectively oversee the Services on an ongoing basis. 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 at our Incidents & the Google Cloud dashboard page. 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.	Business Continuity and Disaster Recovery Significant Developments Data Incidents (Cloud Data Processing Addendum)
18	56 b. identify and manage risks to the APRA-regulated entity that could result from the arrangement, such as step-in risk or contagion risk;	See above. In addition, Google believes in an open cloud that supports multi-cloud and hybrid cloud approaches. If implemented through the use of open-source based technologies, these approaches can provide customers with the levels of portability, substitutability and survivability, required for robust exit planning. Refer to our Strengthening operational resilience in financial services by migrating to Google Cloud whitepaper for more information.	Data Export (Cloud Data Processing Addendum)

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		Google recognizes that, whatever the level of technical resilience that can be achieved on Google Cloud, regulated entities must plan for the scenario in which Google can no longer provide the service. We support such exit plans through: ● Commitment to Open Source: many of our products and services are available in Open Source versions, meaning that they can be run on other Cloud providers or on-premise. ● Commitment to common standards: our platform supports common standards for hosting applications in virtual machines or containers, which can be replicated by alternative services on other Cloud providers or on-premise. ● Anthos multi-Cloud management: our multi-Cloud management product, Anthos, allows customers to run and manage an increasing range of services in the same way as on Google Cloud across other Cloud providers or on-premise. Refer to our Planning for the Worst paper for more information about how Google Cloud supports Reliability, Resilience, Exit and Stressed Exit. Refer to our Engaging in a European dialogue on customer controls and open cloud solutions blog post and our Open Cloud page for more information on our commitment to open source and common standards.	
19	56 c. ensure it can execute its BCP if needed; and	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. Regulated entities can review our plan and testing results. In addition, information about how customers can use our Services in their own business contingency planning is available in our Disaster Recovery Planning Guide.	Business Continuity and Disaster Recovery
20	56 d. ensure it can conduct an orderly exit from the arrangement if needed.	Google recognizes that regulated entities 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 regulated entities achieve this, upon request, Google will continue to provide the Services for 12 months beyond the expiry or termination of the	Transition Term

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		contract. Google will enable you to access and export your data throughout the duration of our contract and during the post-termination transition term. You can export your data from the Services in a number of industry standard formats. For example: ● Google Kubernetes Engine is a managed, production-ready environment that allows portability across different clouds as well as on premises environments. ● Migrate for Anthos allows you to move and convert workloads directly into containers in Google Kubernetes Engine. You can export/import an entire VM image in the form of a .tar archive. Find more information on images here and on storage options here.	Data Export (Cloud Data Processing Addendum)
21	57. APRA may require an APRA-regulated entity to review and make changes to a service provider arrangement where it identifies heightened prudential concerns.	We appreciate 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.	Enabling Customer Compliance