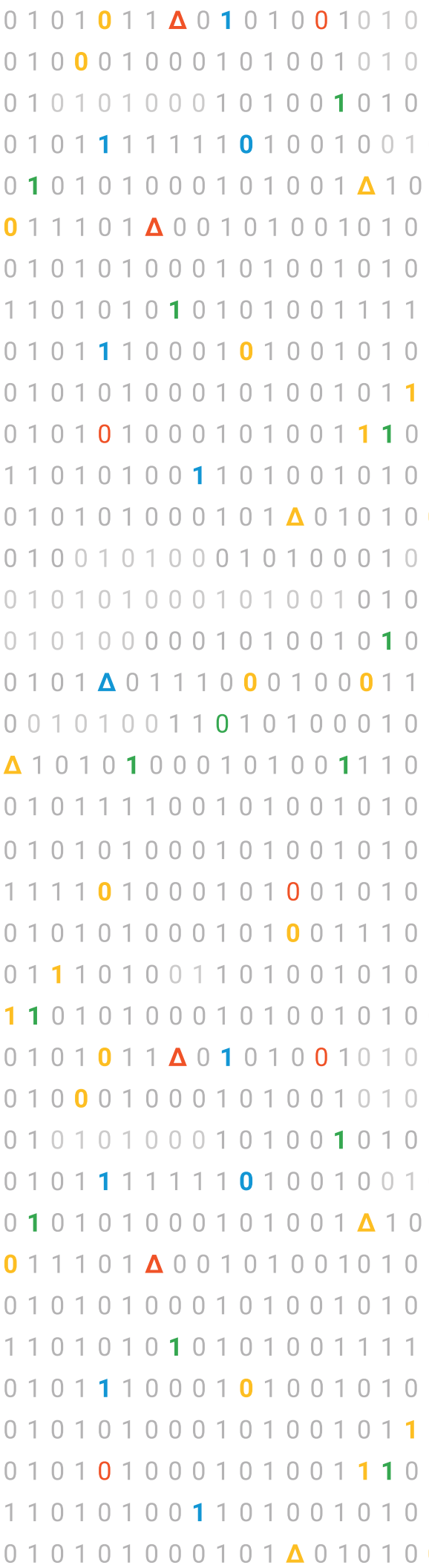
Google Cloud's Response to APRA Prudential Standard

Cloud Whitepaper

January 2018



Google Cloud

Table of Contents

Disclaimer

This document is for informational purposes only. Google does not intend the information or recommendations in this document to constitute legal advice. Each customer must independently evaluate its own particular use of the services as appropriate to support its legal compliance obligations. The content contained herein is correct as of January 2018, and represents the status quo as of the time it was written. This document references, and is limited to, a consideration of Prudential Standard CPS 231, Outsourcing, Version July 2017.

1. Introduction

1.1 Overview

Financial institutions in Australia are increasingly moving to the cloud as a way to effectively manage their digital operations, access new technology, improve security, and achieve cost efficiencies. In order to ensure a high level of information security and management, the Australian Prudential Regulatory Authority (APRA) has released several standards and guidelines that pertain to banks, credit unions, and other financial services institutions (FSIs). The APRA Prudential Standard CPS 231 Outsourcing is one such standard.

This white paper provides general information to financial institutions looking to use Google Cloud services. The discussion is limited to the APRA Prudential Standard CPS 231 Outsourcing, and does not consider any other laws that may be applicable.

2. The Australian Regulation Requirements for FSI

2.1 Are cloud services permitted?

Yes.

The APRA Prudential Standard CPS 231 Outsourcing applies to all outsourcing arrangements involving material business activities, entered into by an APRA-regulated institution and a Head of a group. It requires that such arrangements be subject to appropriate due diligence, approval and ongoing monitoring. All risks arising from outsourcing material business activities must be appropriately managed to ensure that the APRA-regulated institution, or the group it heads, is able to meet its financial and service obligations to its depositors and/or policyholders.

It is for a financial institution to determine whether the required cloud service involves outsourcing a 'material business activity'. If you reach the view that the threshold is not met, the Prudential Standard CPS 231 Outsourcing will not apply.

2.2 What regulations and guidance are relevant?

The APRA website provides links to underlying regulations and guidance including the following standards and practice guides. (You should note that the list below contains some of APRA's publications and does not seek to provide a list of all the guidance or laws that may be applicable to financial institutions).

Regulation	Title
APRA CPS 231	APRA Prudential Standard CPS 231 Outsourcing
APRA SPS 231	APRA Prudential Standard SPS 231 Outsourcing
APRA Information Paper	Outsourcing Involving Shared Computing Services (including Cloud)
APRA CPG-234	CPG 234 – Management of Security Risk in Information and Information Technology
APRA CPG-235	CPG 235 – Managing Data Risk
APRA CPS-232	Prudential Standard CPS 232 Business Continuity Management
APRA CPS-220	Prudential Standard CPS 220 Risk Management
APRA CPS-520	Prudential Standard CPS 520 Fit and Proper

2.3 Is regulatory approval required to move to, or operate in the cloud?

No.

The APRA Prudential Standard CPS 231 Outsourcing does not expressly require regulatory approval. However, financial institutions must adhere to the procedure applicable to all outsourcing of a material business activity, such as consultation and notification with APRA.

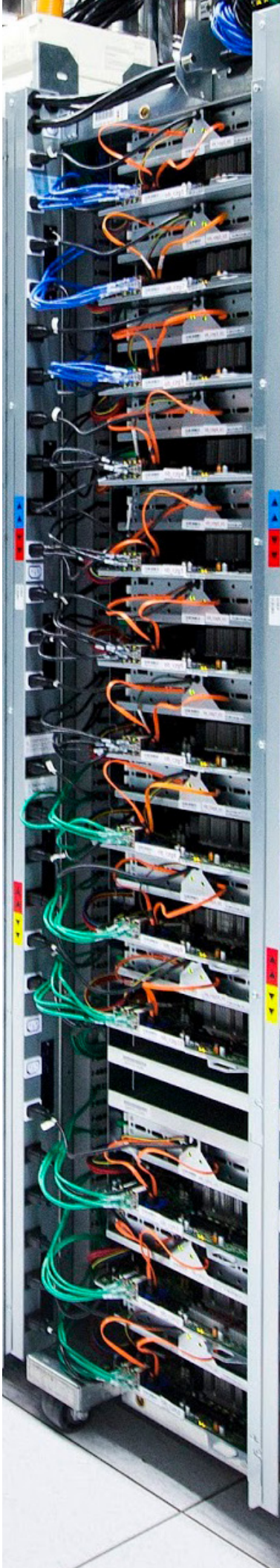
Some examples listed in CPS 231 include:

- maintaining a policy, approved by the Board, relating to outsourcing of material business activities;
- undertaking an assessment process;
- having sufficient monitoring processes in place to manage the outsourcing of material business activities;
- having a legally binding agreement in place, unless otherwise agreed by APRA;
- consulting with APRA prior to entering into agreements to outsource material business activities to service providers that conduct their activities outside Australia; and
- notifying APRA after entering into agreements to outsource material business activities.

2.4 What is a "material business activity"?

Paragraph 14 of the APRA Prudential Standard CPS 231 Outsourcing defines a material business activity as "one that has the potential, if disrupted, to have a significant impact on the APRA-regulated institutions' or group's business operations or its ability to manage risks effectively, having regard to such factors as:

a. the financial and operational impact and impact on reputation of a failure of the service provider to perform over a given period of time;
b. the cost of the outsourcing arrangement as a share of total costs;
c. the degree of difficulty, including the time taken, in finding an alternative service provider or bringing the business activity in-house;
d. the ability of the APRA-regulated institution or member of the group to meet regulatory requirements if there are problems with the service provider;
e. potential losses to the APRA-regulated institutions or group's customers and other affected parties in the event of a service provider failure; and
f. affiliation or other relationship between the APRA-regulated institution or group and the service provider."



2.5 What is "outsourcing"?

Paragraph 10 of the APRA Prudential Standard CPS 231 Outsourcing defines outsourcing as a process which involves "an APRA-regulated institution, or an institution within a group that is not an APRA-regulated institution, entering into an arrangement with another party (including a related body corporate) to perform, on a continuing basis, a business activity that currently is, or could be, undertaken by the institution itself." The standard goes on to say (at paragraph 39) that "an APRA regulated institution must consult with APRA prior to entering any offshoring agreement involving a material business activity so that APRA may satisfy itself that the impact of the offshoring arrangement has been adequately addressed as part of the institution's risk management framework."

Google understands that each customer has unique security and compliance needs. Google Cloud Platform services are available in locations across North America, Europe, and Asia . These locations are subdivided into regions and zones. As a Google Cloud customer, you can deploy your applications so as to best meet your latency, availability and durability requirements. Data locality for Cloud Platform services is governed by the terms of service, including service specific terms.

2.6 Are there any matters that must be addressed in the contract with the service provider?

Where the arrangement is determined by a financial institution to constitute outsourcing of a material business activity, the APRA Prudential Standard CPS 231 Outsourcing provides a list of matters that should be addressed in the outsourcing agreement.

3. Google Cloud Services

3.1 What activities and operations are offered by Google?

Google has two primary cloud offerings, Google Cloud Platform (GCP) and G Suite.

Google Cloud Platform (GCP)
GCP provides Infrastructure as a Service (IaaS) and Platform as a Service (PaaS), allowing businesses and developers to build and run any or all of their applications on Google's Cloud infrastructure. Cloud customers can benefit from performance, scale, reliability, ease-of use, and a pay-as-you-go cost model.

The GCP services that are available are listed below. Each of the services offered as part of GCP has its own options and customisations. For a tailored response, contact the Google Cloud Platform sales team.

Service	Description
Big Data	Tools to capture, process, store, and analyze data on a single platform.
Cloud Management	Manage apps on GCP with a web-based console, mobile app, or Cloud Shell for real time monitoring, logging, diagnostics, and configuration.
Computations	A scalable range of computing options tailored to match the size and needs of an organisation.
Developer Tools	A rich collection of tools and libraries that help development teams work quickly and effectively.
Identity Management Services	Manage the security of and access to cloud assets, supported by Google's own protection of its infrastructure.
Machine Learning	Fast, scalable and easy to use modern machine learning services, with pre-trained models and the ability to generate tailored models.
Networking	A high quality private network using software-defined networking and distributed systems technologies to host and deliver services around the world.
Storage	Scalable storage options and varieties for different needs and price points.

Full details on our GCP services can be found in our Service Organization Controls (SOC3) Service Organization Controls (SOC3) report.

G Suite

G Suite provides Software as a Service (SaaS). The individual products are comprised of communication, productivity, collaboration and security tools that can be accessed from virtually any location with Internet connectivity. This means every employee and each user entity that they work with can be productive from any location, using any device with an Internet connection.

The G Suite services that can be outsourced are listed below. Each of the services offered as part of G Suite has its own options and customisations. For a tailored response, contact our sales team.

Service	Description
Calendar	A cloud-based calendaring service providing web browser and mobile interfaces. Calendar is an application that enables individuals and corporations to coordinate and schedule people, meeting rooms and other resources. Users can create events, send invitations, share schedules and track RSVPs. It is fully integrated with other Google services such as Gmail, Drive, Google+ and Hangout.
Contacts	A cloud-based contacts service providing web browser and mobile interfaces. It allows users to import, store and organize contact information about people and businesses with whom they communicate. Not only can each contact contain basic information such as names, email addresses and phone numbers, they can also include extended information like physical address, employer, department or job title. Users can also create personal groups of contacts to email many people at once. It is fully integrated with other Google services such as Gmail, Drive, Google+ and Groups.
Docs	An online word processor that lets users create and format text documents and collaborate with other users in real time. Documents can be private or shared, and multiple people can edit the same document at the same time. Comments can also be left in the document, and documents can be exported to other file formats.
Drive	A cloud-based storage solution, where users can create, share, collaborate and keep their files. It provides the sharing controls for files and folders, including Google Docs, Sheets and Slides, as well as any other file type. Drive comes with desktop and mobile apps, making it much easier to upload, synchronize and access files from any device. It is fully integrated with other Google services such as Groups, Hangouts and Gmail.
Forms	An online data collection tool that lets users collaboratively build and distribute surveys, polls and quizzes. Forms provides real-time analysis of structured form response data through integration with Google Sheets.
Gmail	A cloud-based email service providing web browser and mobile interfaces. Gmail provides customizable email addresses which include the user entity's own domain, mail search tools and integrated chat. Users can compose and manage email, filter for spam and viruses. It is fully integrated with other Google services such as Calendar, Groups, Google+ and Drive.

Hangouts	A real-time communication and messaging application that allows users to send and receive messages, photos and videos and make one-to-one and group video calls of up to 25 users at a time. It is available on mobile and desktop devices and is fully integrated with Google products such as Gmail, Drive, Google+ and Calendar.
Sheets	An online spreadsheet application that lets users create and format spreadsheets and simultaneously work with other users. Spreadsheets can be private or shared, and multiple people can edit the same spreadsheet at the same time. Comments can also be left in the spreadsheet, and spreadsheets can be exported to other file formats.
Sites	A cloud-based publishing service providing web browser and mobile browser interfaces. It allows the creation of site pages to share and collaborate on documents, videos, schedules and more. It can be published as an internal or an external facing website. It is fully integrated with other Google services such as Drive and Groups.
Slides	An online presentation application that allows users to show off their work in a visual way and present to audiences. Presentations can be private or shared, and multiple people can edit the same presentation at the same time. Comments can also be left in the presentation, and presentations can be exported to other file formats.
Vault	A corporate solution that provides additional storage and searching tools to manage critical information and preserving important corporate data. Vault helps protect user entities with easy-to-use searches so they can quickly find and preserve data to respond to unexpected customer claims, lawsuits or investigations during the electronic discovery (eDiscovery) process. Additionally, Vault gives G Suite user entities the extended management and information governance capabilities to proactively archive, retain and preserve Gmail and on-the-record chats. With the ability to search and manage data based on terms, dates, senders, recipients and labels, Vault helps user entities find the information they need, when they need it.

Further details on our G Suite services can be found in our Service Organization Controls (SOC3) report.

3.2 What data will be processed by the service provider on behalf of the financial institution?

As a GCP or G Suite customer, it is important that you know what data you will be processing when using these services.

GCP

Full details about how data is processed using GCP are provided in our Data Processing and Security Terms and the terms of additional opt-in consents.

G Suite

Full details of how data is processed using G Suite are provided in our Data Processing Amendment.

3.3 How do we seek to address some of your compliance concerns?

One way we demonstrate the reliability of our cloud services is through the independent verification of our security, privacy and compliance controls. Google undergoes several independent third party audits on a regular basis. During these audits an independent auditor examines and certifies the controls present in our data centers, infrastructure and operations. We have regular audits for the following standards:

Service	Description
SSAE16 / ISAE 3042 Type II	• SOC1 • SOC2 • SOC 3 public audit report
ISO 27001	One of the most widely recognized, internationally accepted independent security standards. Google has earned ISO 27001 certification for the systems, applications, people, technology, processes and data centers serving Google Cloud Platform. • ISO 27001 for Google Cloud Platform • ISO 27001 for Google's shared Common Infrastructure

ISO 27017 Cloud Security	An international standard of practice for information security controls based on ISO/IEC 27002 specifically for cloud services. • ISO 27017 for Google Cloud Platform
ISO 27018 Cloud Privacy	An international standard of practice for the protection of personally identifiable information (PII) in public cloud services. • ISO 27018 for Google Cloud Platform
PCI DSS v3.2	The Payment Card Industry (PCI) Security Standards Council was established by the major credit card companies as a separate global organisation to define appropriate practices that merchants and service providers should follow to protect payment cardholder data. The PCI Security Standards Council created the PCI Data Security Standard (DSS) to define a global information security standard for the protection of payment cardholder data. For more information on how GCP meets the requirements for PCI DSS, see our compliance website.

Our third party audit approach is designed to be comprehensive in order to provide assurances of Google's level of information security with regard to confidentiality, integrity and availability. Our customers can use these third party audits to assess how our products can meet their compliance and data-processing needs. Further details about our compliance program can be found in our compliance overview.

For our financial service customers, we can provide specific terms under the Google Cloud Financial Services addendum. This addendum is available, on request, during the contracting phase with Google.

4. Customer Responsibilities

The APRA Prudential Standard CPS 231 Outsourcing requires that financial institutions have internal mechanisms and controls in place to properly manage any outsourcing arrangements. Implementing the recommendations of the guidelines is primarily the responsibility of each individual financial institution. The table below lists some of the key requirements of APRA Prudential Standard CPS 231 Outsourcing. The requirements listed below should not be considered exhaustive of your obligations. You should, as always, perform due diligence to ensure you cover all of the requirements of APRA Prudential Standard CPS 231 Outsourcing, as well as any other APRA guidelines and other applicable financial services laws.

Customer Requirement	This Document
Assessment of outsourcing options	Section 4.1
Outsourcing policy	Section 4.2
The role of the Board and senior management	Section 4.3
Monitoring the relationship	Section 4.4
The outsourcing agreement	Section 4.5
APRA access to service providers	Section 4.6

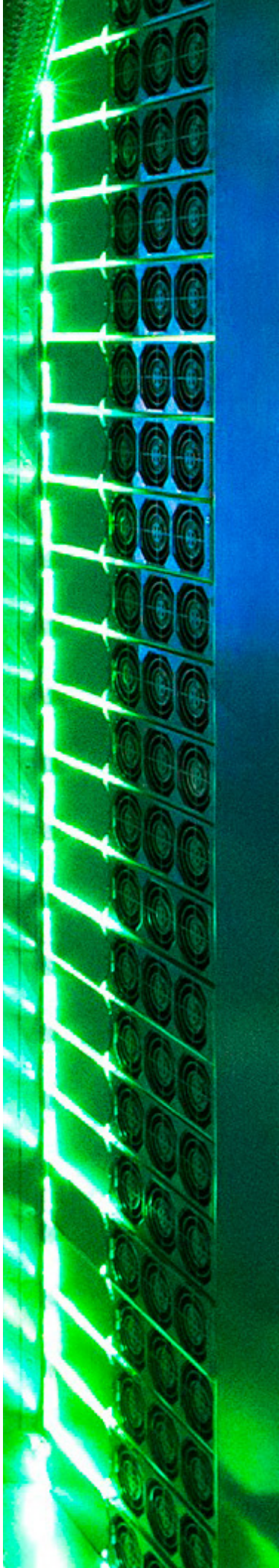
4.1 Assessment of outsourcing options

Paragraph 26 of the APRA Prudential Standard CPS 231 Outsourcing requires that you, the customer, be able to demonstrate to APRA that, in assessing the options for outsourcing a material business activity to a third party, you have undertaken the steps listed below. As always, please consult your own independent legal advisors for development of your compliance plans.

a. Prepare a business case for outsourcing the material business activity.
b. Undertake a tender or other selection process for selecting the service provider.
c. Undertake a due diligence review of the chosen service provider, including the ability of the service provider to conduct the business activity on an ongoing basis.
d. Involve the Board of the APRA-regulated institution, Board committee of the APRA-regulated institution, or senior manager of the institution with delegated authority from the Board, in approving the agreement.
e. Consider all the matters outlined in paragraph 29, that must, at a minimum, be included in the outsourcing agreement itself.
f. Establish procedures for monitoring performance under the outsourcing agreement on a continuing basis.
g. Address the renewal process for outsourcing agreements and how the renewal will be conducted.
h. Develop contingency plans that would enable the outsourced business activity to be provided by an alternative service provider or brought in-house if required.

The Google team can provide you with further materials to assist your independent legal and compliance development plans. These materials include audit reports, service documentation, control mappings, and other relevant whitepapers. If you need assistance with this requirement, contact our Cloud Sales team.

For more information, see the resources listed below.



Resources	Description
GCP platform overview	A high-level, technical look at how the Cloud Platform works.
GCP product documentation	Comprehensive product site that provides detailed service definitions, use cases and technical How-to guides.
GCP data processing and security terms	Detailed data process and security terms for GCP services.
GCP's security model and compliance program	An overview of GCP's security model and compliance certifications.
G Suite overview	A high-level overview of G Suite features.
G Suite solutions for business	Detailed solutions for small, midsize and large business.
G Suite data processing amendment	Detailed data processing terms for G Suite services
G Suite's security model and compliance program	An overview of G Suite's security model and compliance certifications.

4.2 Outsourcing policy

Do you have a policy, approved by the Board, relating to outsourcing?

While Google cannot prescribe such a policy, we encourage our customers to take into consideration all of the requirements outlined in the APRA Prudential Standard CPS 231 Outsourcing and associated practice guide. The full text of this requirement can be found in paragraphs 23 - 25 of APRA Prudential Standard CPS 231 Outsourcing.

4.3 The role of the Board and senior management

What procedures do you have in place to ensure that all your relevant business units are fully aware of, and comply with, your outsourcing policy?

Google cannot prescribe the procedures that you should have in place to ensure that your relevant business units are within the scope of your outsourcing policy. We do however recommend that you document any and all such procedures in your outsourcing policy. The full text of this requirement can be found in paragraph 21 of APRA Prudential Standard CPS 231 Outsourcing.

How do you ensure that you maintain ultimate responsibility for any outsourcing?

Paragraph 22 of APRA Prudential Standard CPS 231 Outsourcing, states that you, the customer, are ultimately responsible for complying with all prudential responsibilities relating to any outsourced business activity.

4.4 Monitoring the Relationship

What monitoring processes do you have in place to manage outsourcing?

Paragraph 41 of APRA Prudential Standard CPS 231 Outsourcing requires that you must ensure that you have "sufficient and appropriate resources to manage and monitor each outsourcing relationship at all times. The type and extent of resources required will depend on the materiality of the outsourced business activity. At a minimum, monitoring must include:

a. maintaining appropriate levels of regular contact with the service provider. This will range from daily operational contact to senior management involvement; and
b. a process for regular monitoring of performance under the agreement, including meeting criteria concerning service levels."

At Google, we have customer support specialists that can assist with this requirement. GCP has a customer console that makes the monitoring process easier for you. The console contains service health dashboards that allow you to see, in real time, information about your service such as availability, details on any service disruptions, and scheduled maintenance. In addition to the customer console, you can also request copies of the certification that Google receives that prove compliance with international standards:

- Google's ISO certification is available from our compliance page
- Google's SOC report can be obtained from your account representative.

Paragraph 42 of APRA Prudential Standard CPS 231 Outsourcing requires that you "must advise APRA of any significant problems that have the potential to materially affect the outsourcing arrangement and, as a consequence, materially affect [your] business operations, profitability or reputation."

Paragraph 43 of APRA Prudential Standard CPS 231 Outsourcing requires that "where an outsourcing agreement is terminated, an APRA-regulated institution must notify APRA as soon as practicable and provide a statement about the transitional arrangements and future strategies for carrying out the outsourced material business activity."

Further details on ownership of the documents, records, software and hardware, and your role when transitioning out of the Google service in the event of termination of an agreement can be found in the applicable terms of service.

4.5 The outsourcing agreement

Paragraph 28 of APRA Prudential Standard CPS 231 Outsourcing provides that, except where otherwise stated in the standard, "each outsourcing arrangement must be contained in a documented legally binding agreement. The agreement must be signed by all parties before the outsourcing arrangement begins."

You can find examples of Google's standard terms for customers who purchase from Google at: GCP terms of service and G Suite Term of Service.

In addition, we can offer additional terms in a Google Cloud Financial Services addendum for financial services customers. This is available from your sales representative at any time on request and will be presented to you before you enter into any legally binding agreement.

4.6 APRA access to service providers

Paragraph 34 of APRA Prudential Standard CPS 231 Outsourcing requires that your outsourcing agreement "must include a clause that allows APRA access to documentation and information relating to the outsourcing arrangement." At APRA's request, we will provide APRA with the SOC 2 report as defined in our Data Processing and Security Terms.