APRA Prudential Standard CPS 234 Information Security

Google Cloud Mapping

This document is designed to help financial institutions supervised by the Australian Prudential Regulation Authority ("**APRA**") to consider Prudential Standard CPS 234 Information Security ("**framework**") in the context of Google Cloud Platform ("**GCP**") and the Google Cloud Financial Services contract.

We focus on the following requirements of the framework: Information Security Capability, Policy Framework, Information asset identification and classification, Implementation of Controls, Incident Management, Testing Control Effectiveness, Internal Audit and APRA Notification (Paragraphs 15 - 36). 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	**Information security capability**		
2	15. An APRA-regulated entity must maintain an information security capability commensurate with the size and extent of threats to its information assets, and which enables the continued sound operation of the entity.	This is a customer consideration. See Row 3 for information about Google's security capability.	N/A
3	16. Where information assets are managed by a related party or third party, the APRA-regulated entity must assess the information security capability of that party, commensurate with the potential consequences of an information security incident affecting those assets.	The 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 Cloud Data Processing Addendum. 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 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:	Data Security; Security Measures (Cloud Data Processing Addendum)

APRA Prudential Standard CPS 234 Information Security

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		• **Encryption at rest.** Google encrypts customer data stored at rest by default, with no additional action required from you. More information is available at: https://cloud.google.com/security/encryption-at-rest/default-encryption. • **Encryption in transit.** Google encrypts and authenticates all data in transit at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. More information is available at https://cloud.google.com/security/encryption-in-transit. (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	
4	17. An APRA-regulated entity must actively maintain its information security capability with respect to changes in vulnerabilities and threats, including those resulting from changes to information assets or its business environment.	Customers are responsible for vulnerability management within their accounts and hosted solutions, while Google safeguards the overall security of Google Cloud services. 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 here. Here are some examples: • **Cloud Identity and Access Management** helps to prevent against unauthorized access by controlling access rights and roles for Google Cloud Platform resources. • **Cloud Security Scanner** automatically scans App Engine, Compute Engine, and Google Kubernetes Engine apps for common vulnerabilities.	N/A

APRA Prudential Standard CPS 234 Information Security

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference

		• **Event Threat Detection** automatically scans various types of logs for suspicious activity in your Google Cloud Platform environment.
		
		• **Cloud Security Command Center** and **Security Health Analytics** provide visibility and monitoring of Google Cloud Platform resources and changes to resources including VM instances, images, and operating systems.
		
		• **Forseti** is an open source toolkit designed to help give your security teams the confidence and peace of mind that they have the appropriate security controls in place across our services. Forseti includes the following security tools:
		  ○ Inventory: provides visibility into existing GCP resources
		  ○ Scanner: validates access control policies across GCP resources
		  ○ Enforcer: removes unwanted access to GCP resources
		  ○ Explain: analyzes who has what access to GCP resources.
		
		For more information, see here.
		
		For its part, Google's threat detection systems are constantly updated based on attack signatures encountered.
		
		Google performs periodic network vulnerability scans, application-layer vulnerability scans, and local operating system-layer scans and checks using commercial and proprietary tools. More information is available in Google's CSA Star SOC2+ report.	

5	**Policy Framework**		
6	18. An APRA-regulated entity must maintain an information security policy framework commensurate with its exposures to vulnerabilities and threats	This is a customer consideration. Refer to Row 4 for more information about the tools Google provides to help you enhance and monitor the security of your data.	N/A
7	19. An APRA-regulated entity's information security policy framework must provide direction on the responsibilities of all parties who have an obligation to maintain information security	Google's responsibilities for the security of the services and customer data are described in the Cloud Data Processing Addendum where Google makes commitments to protect your data, including regarding security, deletion, access and transfer.	Data Security; Security Measures (Cloud Data Processing Addendum)
8	**Information asset identification and classification**		
9	20. An APRA-regulated entity must classify its information assets, including those managed by related parties and third parties, by criticality and sensitivity. This classification must reflect the degree to which an information security incident affecting an information asset has the potential to affect, financially or non financially, the entity or the interests of depositors, policyholders, beneficiaries or other customers	The GCP 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 which information assets are managed by the services. Customers may leverage Cloud Asset Inventory to view, monitor, and analyze all of their GCP assets.	N/A

APRA Prudential Standard CPS 234 Information Security

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		For its part, Google maintains assets inventories and assigns ownership for managing its critical resources. Google also tags physical hardware. Components are inventoried for easy identification and tracking within Google facilities. Other hardware characteristics, such as MAC are used for identification. More information is available in Google's CSA Star SOC2+ report.	
10	**Implementation of controls**		
11	21. An APRA-regulated entity must have information security controls to protect its information assets, including those managed by related parties and third parties, that are implemented in a timely manner and that are commensurate with: (a) vulnerabilities and threats to the information assets; (b) the criticality and sensitivity of the information assets; (c) the stage at which the information assets are within their life-cycle; and (d) the potential consequences of an information security incident.	Google recognizes that customers need to review our internal controls as part of their information security and risk assessment. To assist, Google undergoes several independent third-party audits on at least an annual basis to provide independent verification of our operations and internal controls. 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.	Certifications and Audit Reports
12	22. Where an APRA-regulated entity's information assets are managed by a related party or third party, the APRA-regulated entity must evaluate the design of that party's information security controls that protects the information assets of the APRA-regulated entity	Refer to Row 3 and 11 for more information on how you can evaluate Google's information security controls.	N/A
13	**Incident management**		
14	23. An APRA-regulated entity must have robust mechanisms in place to detect and respond to information security incidents in a timely manner	Refer to Row 4 for more information about the tools Google provides to help you enhance and monitor the security of your data. In addition, 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 here. 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 (Cloud Data Processing Addendum)

APRA Prudential Standard CPS 234 Information Security

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
15	24. An APRA-regulated entity must maintain plans to respond to information security incidents that the entity considers could plausibly occur (information security response plans).	Refer to Row 14.	N/A
16	25. An APRA-regulated entity's information security response plans must include the mechanisms in place for: (a) managing all relevant stages of an incident, from detection to post-incident review; and (b) escalation and reporting of information security incidents to the Board, other governing bodies and individuals responsible for information security incident management and oversight, as appropriate.	Refer to Row 14	N/A
17	26. An APRA-regulated entity must annually review and test its information security response plans to ensure they remain effective and fit-for-purpose.	Google performs tests of its incident response processes and procedures for key areas, such as systems that store customer data. These tests take into consideration a variety of scenarios, including insider threats and software vulnerabilities and help us better prepare for security and privacy incidents. More information on Google's data incident response process is available in our Data incident response whitepaper.	N/A
18	**Testing control effectiveness**		
19	27. An APRA-regulated entity must test the effectiveness of its information security controls through a systematic testing program. The nature and frequency of the systematic testing must be commensurate with: (a) the rate at which the vulnerabilities and threats change; (b) the criticality and sensitivity of the information asset; (c) the consequences of an information security incident; d) the risks associated with exposure to environments where the APRA regulated entity is unable to enforce its information security policies; and (e) the materiality and frequency of change to information assets	This is a customer consideration.	N/A
20	28. Where an APRA-regulated entity's information assets are managed by a related party or a third party, and the APRA-regulated entity is reliant on that party's information security control testing, the APRA-regulated entity must assess whether the nature and frequency of testing of controls in respect of those information assets is commensurate with paragraphs 27(a) to 27(e) of this Prudential Standard.	Refer to Row 11 for more information on the independent third-party audits Google undergoes to provide independent verification of our operations and internal controls Google is audited at least once a year for each audited framework. Audits include testing of operational effectiveness of key controls in place. As part of Google's routine planning, scoping, and readiness activities, recurring key systems and controls, as well as new systems and controls, are reviewed prior to the audit work commencing. In addition, Google recognizes that regulated entities may wish to audit the services operations and controls directly. Google grants audit rights to regulated entities and their independent auditors.	Certifications and Audit Reports Enabling Customer Compliance
21	29. An APRA-regulated entity must escalate and report to the Board or senior management any testing results that identify information security control deficiencies that cannot be remediated in a timely manner.	This is a customer consideration.	N/A
22	30. An APRA-regulated entity must ensure that testing is conducted by appropriately skilled and functionally independent specialists.	Google engages certified and independent third party auditors for each audited framework. Refer to the relevant certification or audit report for information on the	N/A

APRA Prudential Standard CPS 234 Information Security

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		certifying or auditing party. Refer to Row 11 for the information about the certification and audit reports Google maintains.	
23	31. An APRA-regulated entity must review the sufficiency of the testing program at least annually or when there is a material change to information assets or the business environment.	Google is audited at least once a year for each audited framework. Refer to Row 11 for the information about the certification and audit reports Google maintains.	Certifications and Audit Reports
24	**APRA Notification**		
25	35. An APRA-regulated entity must notify APRA as soon as possible and, in any case, no later than 72 hours, after becoming aware of an information security incident that: (a) materially affected, or had the potential to materially affect, financially or non-financially, the entity or the interests of depositors, policyholders, beneficiaries or other customers; or (b) has been notified to other regulators, either in Australia or other jurisdictions.	Google will notify you of data incidents promptly and without undue delay. Google's notification will describe, to the extent possible, the nature of the data incident, the measures taken to mitigate the potential risks and the measures Google recommends customers take to address the data incident. After being made aware of a data incident by Google, regulated entities may use the information provided by Google together with the information available to the regulated entity internally (e.g. impact of the incident) to determine if a notification to APRA is required and do so within the requisite time frame. More information on Google's data incident response process is available in our Data incident response whitepaper.	Data Incidents (Cloud Data Processing Addendum)
26	36. An APRA-regulated entity must notify APRA as soon as possible and, in any case, no later than 10 business days, after it becomes aware of a material information security control weakness which the entity expects it will not be able to remediate in a timely manner.	Remediation is a key phase of Google's incident response process. The focus of this phase is investigating the root cause of the data incident, limiting the impact of the incident, resolving immediate security risks (if any), implementing necessary fixes as part of remediation, and recovering affected systems, data, and services. Following the successful remediation and resolution of a data incident, the incident response team evaluates the lessons learned from the incident. If follow-up work is required, the incident response team develops an action plan to complete that work and assigns project managers to spearhead the long-term effort. The incident is closed after the remediation efforts conclude. To the extent possible, Google's customer notification will describe the measures taken to mitigate the potential risks and the measures Google recommends customers take to address the data incident. More information on Google's data incident response process is available in our Data incident response whitepaper.	Significant Developments Data Incidents (Cloud Data Processing Addendum)