Google Cloud Platform: Customer Responsibility Matrix

December 2018

Google Cloud Platform

Introduction

Google Cloud Platform (GCP) was designed with security as a core design component. Google uses a variety of technologies and processes to secure information stored on Google servers. Google has performed independent validation on Payment Card Industry Data Security Standard (PCI DSS) requirements that apply to GCP technologies and infrastructure managed by Google. Google offers customers a great deal of control over their instances running on Google's infrastructure. Google does not control security on the operating system, packages or applications that are deployed by customers on GCP. It is the customer's responsibility to comply with requirements of PCI DSS that relate to operating systems packages and applications deployed by customer.

GCP adheres to the PCI DSS requirements set forth for a level 1 Service Provider. GCP is required to be compliant with PCI DSS and all applicable requirements that directly apply to a service provider. This document outlines each requirement that Google complies with on behalf customers who use GCP to deliver PCI-compliant products and services . If a requirement is not included in this document, that indicates that GCP is not performing the requirement on behalf of its clients. With respect to the cloud hosting services which GCP delivers to its Customers, responsibility for the various requirements associated with PCI DSS varies. Some requirements are the sole responsibility of GCP, some requirements are the sole responsibility of the Customer, and some requirements are a shared responsibility between both parties.

We recommend that Customers reference the responsibility matrix in this document as they pursue PCI compliance and find it a useful tool when conducting their own PCI audits.

Definitions

Term	Description
Google	The service provider
Google Cloud Platform (GCP) responsibility	**The requirement in question is the responsibility of, and implemented by, Google.** A Qualified Security Assessor has assessed and validated these requirements and found GCP to be compliant with PCI-DSS v3.2. These requirements, which support the Customer's PCI-DSS efforts but the Customer cannot manage directly, are the sole responsibility of GCP
Customer responsibility	**The requirement in question is the responsibility of, and implemented by, the customer.** These requirements were not applicable to Google Cloud services as they are designed and these are the customer responsibilities. Customers of GCP bear sole responsibility to meet their own PCI DSS compliance for these requirements.
Shared responsibility	**Both the customer and Google are responsible for implementing parts of the requirement.** A Qualified Security Assessor has assessed and validated these specific requirements and found GCP to be compliant with PCI-DSS v3.2. However, Customers of GCP share some responsibility and must take action in order to meet their own PCI DSS compliance for these requirements.
Service Provider	The Service Provider, as defined by the requirement, is Google
POS	Point of Sale
PCI DSS	Payment Card Industry Data Security Standard

PCI DSS Responsibility Matrix

Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data

Requirement	Description	GCP	Customer
1.1	**Establish and implement firewall and router configuration standards that include the following:**	Google's internal production network and systems have been assessed against and comply with this requirement.	GCP customers are responsible for implementing the processes and procedures necessary to ensure that all network connections, inbound and outbound traffic on any customer instances deployed on GCP comply with the requirements of section 1 of the PCI DSS
1.1.1	A formal process for approving and testing all network connections and changes to the firewall and router configurations.	Google's internal production network and systems have been assessed against and comply with this requirement.	GCP customers are responsible for implementing the processes and procedures necessary to ensure that all network connections, inbound and outbound traffic on any customer instances deployed on GCP comply with the requirements of section 1 of the PCI DSS
1.1.2	Current diagram that identifies all networks, network devices, and system components, with all connections between the CDE and other networks, including any wireless networks.	Google's internal production network and systems have been assessed against and comply with this requirement.	GCP customers are responsible for implementing the processes and procedures necessary to ensure that all network connections, inbound and outbound traffic on any customer

			instances deployed on GCP comply with the requirements of section 1 of the PCI DSS
1.1.3	Current network diagram that shows all cardholder data flows across systems and networks.	Google's internal production network and systems have been assessed against and comply with this requirement.	GCP customers are responsible for implementing the processes and procedures necessary to ensure that all network connections, inbound and outbound traffic on any customer instances deployed on GCP comply with the requirements of section 1 of the PCI DSS
1.1.4	Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone.	Firewalls that comply with this requirement have been implemented by Google to control access to the Google production network and to GCP products and services implemented by Google.	GCP customers are responsible for implementing the processes and procedures necessary to ensure that all network connections, inbound and outbound traffic on any customer instances deployed on GCP comply with the requirements of section 1 of the PCI DSS
1.1.5	Description of groups, roles, and responsibilities for management of network components.	Google's internal production network and systems have been assessed against and comply with this requirement.	GCP customers are responsible for implementing the processes and procedures necessary to ensure that all network connections, inbound and outbound traffic on any customer instances deployed on GCP comply with the requirements of section 1 of the PCI DSS

1.1.6	Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure. Examples of insecure services, protocols, or ports include but are not limited to FTP, Telnet, POP3, IMAP, and SNMP v1 and v2.	Firewalls that comply with this requirement have been implemented by Google to control access to the Google production network and to GCP products and services implemented by Google.	GCP customers are responsible for implementing the processes and procedures necessary to ensure that all network connections, inbound and outbound traffic on any customer instances deployed on GCP comply with the requirements of section 1 of the PCI DSS
1.1.7	Requirement to review firewall and router rule sets at least every six months.	Firewalls that comply with this requirement have been implemented by Google to control access to the Google production network and to GCP products and services implemented by Google.	GCP customers are responsible for implementing the processes and procedures necessary to ensure that all network connections, inbound and outbound traffic on any customer instances deployed on GCP comply with the requirements of section 1 of the PCI DSS
1.2	**Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.**		
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	Firewalls that comply with this requirement have been implemented by Google to control access to the Google production network and to GCP products and services implemented by Google.	GCP customers are responsible for ensuring that firewalls that meet Section 1 requirements are implemented on inbound and outbound traffic, to and from any customer instances deployed on GCP meet the requirements of Section 1 of the PCI DSS. Refer to the Google Compute

			Engine documentation for the capabilities provided by GCP to the customer.
1.2.2	Secure and synchronize router configuration files.	Google's internal production network and systems have been assessed against and comply with this requirement.	GCP customers are responsible for ensuring that firewalls meeting Section 1 requirements are implemented on inbound and outbound traffic, to and from any customer instances deployed on GCP meet the requirements of Section 1 of the PCI DSS. Refer to the Google Compute Engine documentation for the capabilities provided by GCP to the customer.
1.2.3	Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.	Firewalls that comply with this requirement have been implemented by Google to control access to the Google production network and to GCP products and services implemented by Google.	GCP customers are responsible for ensuring that firewalls meeting Section 1 requirements are implemented on inbound and outbound traffic, to and from any customer instances deployed on GCP meet the requirements of Section 1 of the PCI DSS. Refer to the Google Compute Engine documentation for the capabilities provided by GCP to the customer.
1.3	**Prohibit direct public access between the Internet and any system component in the cardholder data environment.**		
1.3.1	Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	Firewalls that comply with this requirement have been implemented by Google to control access to the Google	GCP customers are responsible for ensuring that firewalls meeting Section 1 requirements are implemented on inbound

		production network and to GCP products and services implemented by Google.	and outbound traffic, to and from any customer instances deployed on GCP meet the requirements of Section 1 of the PCI DSS. Refer to the Google Compute Engine documentation for the capabilities provided by GCP to the customer.
1.3.2	Limit inbound Internet traffic to IP addresses within the DMZ.	Firewalls that comply with this requirement have been implemented by Google to control access to the Google production network and to GCP products and services implemented by Google.	GCP customers are responsible for ensuring that firewalls meeting Section 1 requirements are implemented on inbound and outbound traffic, to and from any customer instances deployed on GCP meet the requirements of Section 1 of the PCI DSS. Refer to the Google Cloud Platform (GCP) firewall rules documentation for the capabilities provided by GCP to the customer.
1.3.3	Implement anti—spoofing measures to detect and block forged source IP addresses from entering the network.	Firewalls that comply with this requirement have been implemented by Google to control access to the Google production network and to GCP products and services implemented by Google.	GCP customers are responsible for ensuring that firewalls meeting Section 1 requirements are implemented on inbound and outbound traffic, to and from any customer instances deployed on GCP meet the requirements of Section 1 of the PCI DSS.
1.3.4	Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	Firewalls that comply with this requirement have been implemented by Google to control access to the Google production network and to GCP products and services implemented by Google.	GCP customers are responsible for ensuring that firewalls meeting Section 1 requirements are implemented on inbound and outbound traffic, to and from any customer instances deployed on GCP

			meet the requirements of Section 1 of the PCI DSS.
1.3.5	Permit only “established” connections into the network.	Firewalls that comply with this requirement have been implemented by Google to control access to the Google production network and to GCP products and services implemented by Google.	GCP customers are responsible for ensuring that firewalls meeting Section 1 requirements are implemented on inbound and outbound traffic, to and from any customer instances deployed on GCP meet the requirements of Section 1 of the PCI DSS. Refer to the Google Cloud Platform (GCP) firewall rules documentation for the capabilities provided by GCP to the customer.
1.3.6	Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	Firewalls that comply with this requirement have been implemented by Google to control access to the Google production network and to GCP products and services implemented by Google.	GCP customers are responsible for ensuring that firewalls meeting Section 1 requirements are implemented on inbound and outbound traffic, to and from any customer instances deployed on GCP meet the requirements of Section 1 of the PCI DSS. Refer to the Google Cloud Platform (GCP) firewall rules documentation for the capabilities provided by GCP to the customer.
1.3.7	Do not disclose private IP addresses and routing information to unauthorized parties. Note: Methods to obscure IP addressing may include, but are not limited to: ● Network Address Translation (NAT).	Google has PCI DSS compliance responsibility for dedicated internal Google Production and management network systems. For computer resources that are provided by Google to customers as part of a customer's GCP project, the PCI	GCP customers are responsible for ensuring that firewalls meeting Section 1 requirements are implemented on inbound and outbound traffic, to and from any customer instances deployed on GCP meet the requirements of Section 1 of the

	• Placing servers containing cardholder data behind proxy servers/firewalls . • Removal or filtering of route advertisements for private networks that employ registered addressing. • Internal use of RFC1918 address space instead of registered addresses.	compliance of those resources is the customer's responsibility.	PCI DSS. Refer to the Google Cloud Platform (GCP) firewall rules documentation for the capabilities provided by GCP to the customer.
1.4	**Install personal firewall software on any mobile and/or employee owned devices that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the network.**	This requirement was determined as out of scope by the QSA for Google Cloud PCI Assessment.	GCP customers are responsible for ensuring that devices or systems that fall within the scope of this requirement are compliant.
1.5	**Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties.**	This requirement was determined as out of scope by the QSA for Google Cloud PCI Assessment.	GCP customers are responsible for ensuring that devices or systems that fall within the scope of this requirement are compliant.

Requirement 2: Do Not Use Vendor Supplied Defaults for System Passwords and Other Security

Requirement	Description	GCP	Customer
2.1	**Always change vendor supplied defaults and remove or disable unnecessary default accounts before installing a system on the network.**	Google has PCI DSS compliance responsibility for dedicated internal Google Production and management network systems.	For computer resources that are provided by Google to customers as part of a customer's GCP project the PCI compliance of those resources is the customer's responsibility.
2.1.1	For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.	No wireless networks are connected to the Cardholder Data Environment relating to GCP.	GCP customers are responsible for complying with this requirement for any wireless network that may fall within the scope of their PCI DSS assessments.
2.2	**Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry- accepted system hardening standards.**	Google has implemented configuration standards that comply with requirements in section 2.2 for the infrastructure underlying GCP products in scope for PCI.	GCP customers are responsible for complying with this requirement for any virtual machines, applications, services or databases deployed by them on GCP.
2.2.1	Implement only one primary function per server to prevent functions that require different security levels from coexisting on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.)	Google has implemented configuration standards that comply with requirements in section 2.2 for the infrastructure underlying GCP products in scope for PCI.	GCP customers are responsible for complying with this requirement for any virtual machines, applications, services or databases deployed by them on GCP.

2.2.2	Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	Google has implemented configuration standards that comply with requirements in section 2.2 for the infrastructure underlying GCP products in scope for PCI.	GCP customers are responsible for complying with this requirement for any virtual machines, applications, services or databases deployed by them on GCP.
2.2.3	Implement additional security features for any required services, protocols, or daemons that are considered to be insecure—for example, use secured technologies such as SSH, SFTP, TLS or IPSec VPN to protect insecure services such as NetBIOS, file sharing, Telnet, FTP, etc.	Google has implemented configuration standards that comply with requirements in section 2.2 for the infrastructure underlying GCP products in scope for PCI.	GCP customers are responsible for complying with this requirement for any virtual machines, applications, services or databases deployed by them on GCP.
2.2.4	Configure system security parameters to prevent misuse.	Google has implemented configuration standards that comply with requirements in section 2.2 for the infrastructure underlying GCP products in scope for PCI.	GCP customers are responsible for complying with this requirement for any virtual machines, applications, services or databases deployed by them on GCP.
2.2.5	Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	Google has implemented configuration standards that comply with requirements in section 2.2 for the infrastructure underlying GCP products in scope for PCI.	GCP customers are responsible for complying with this requirement for any virtual machines, applications, services or databases deployed by them on GCP.
2.3	**Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or TLS for web-based management and other non-console administrative access.**	Google has implemented controls for secure administrative access for the Google production infrastructure underlying GCP.	GCP customers are responsible for complying with this requirement for any virtual machines, applications, services or databases deployed by them on GCP.

2.4	**Maintain an inventory of system components that are in scope for PCI DSS.**	Google has implemented policies and procedures that comply with requirements in section 2.4 for the infrastructure underlying GCP products in scope for PCI.	GCP customers are responsible for complying with this requirement for any virtual machines, applications, services or databases deployed by them on GCP.
2.5	**Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.**	Google has implemented policies and procedures that comply with requirements in section 2.5 for the infrastructure underlying GCP products in scope for PCI.	GCP customers are responsible for complying with this requirement for any virtual machines, applications, services or databases deployed by them on GCP.
2.6	**Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers.**	Compliance Covered in Appendix-A Controls Section.	N/A

Requirement 3: Protect Stored Cardholder Data

Requirement	Description	GCP	Customer
3.1	**Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage:** ● **Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements** ● **Processes for secure deletion of data when no longer needed** ● **Specific retention requirements for cardholder data** ● **A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.**	It is outside the the scope of Google's PCI assessment to comply with requirements of section 3 for cardholder data stored within any customer instances on GCP.	GCP customers are responsible for meeting the requirements of section 3 for any cardholder data transmitted to or stored within their instances, applications or databases on GCP.
3.2	**Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process. It is permissible for issuers and companies that support issuing services to store sensitive authentication data if: There is a business justification and The data is stored securely.**	Google has PCI DSS compliance responsibility for dedicated internal Google Production and management network systems. For computer resources that are provided by Google to customers as part of a customer's GCP project. the PCI compliance of those resources is the customer's responsibility.	GCP customers are responsible for meeting the requirements of section 3 for any cardholder data transmitted to or stored within their instances, applications or databases on GCP.

3.2.1	Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic stripe data.	It is outside the the scope of Google's PCI assessment to comply with requirements of section 3 for cardholder data stored within any customer instances on GCP.	GCP customers are responsible for meeting the requirements of section 3 for any cardholder data transmitted to or stored within their instances, applications or databases on GCP.
3.2.2	Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card not present transactions.	It is outside the the scope of Google's PCI assessment to comply with requirements of section 3 for cardholder data stored within any customer instances on GCP.	GCP customers are responsible for meeting the requirements of section 3 for any cardholder data transmitted to or stored within their instances, applications or databases on GCP.
3.2.3	Do not store the personal identification number (PIN) or the encrypted PIN block.	It is outside the the scope of Google's PCI assessment to comply with requirements of section 3 for cardholder data stored within any customer instances on GCP.	GCP customers are responsible for meeting the requirements of section 3 for any cardholder data transmitted to or stored within their instances, applications or databases on GCP.
3.3	**Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see the full PAN.**	It is outside the the scope of Google's PCI assessment to comply with requirements of section 3 for cardholder data stored within any customer instances on GCP.	GCP customers are responsible for meeting the requirements of section 3 for any cardholder data transmitted to or stored within their instances, applications or databases on GCP.
3.4	**Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches:**	It is outside the the scope of Google's PCI assessment to comply with requirements of section 3 for cardholder data stored	GCP customers are responsible for meeting the requirements of section 3 for any cardholder data transmitted to or

	• **One way hashes based on strong cryptography (hash must be of the entire PAN).** • **Truncation (hashing cannot be used to replace the truncated segment of PAN)** • **Index tokens and pads (pads must be securely stored)** • **Strong cryptography with associated key management processes and procedures.**	within any customer instances on GCP.	stored within their instances, applications or databases on GCP.
3.4.1	If disk encryption is used (rather than file or column level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.	It is outside the the scope of Google's PCI assessment to comply with requirements of section 3 for cardholder data stored within any customer instances on GCP.	GCP customers are responsible for meeting the requirements of section 3 for any cardholder data transmitted to or stored within their instances, applications or databases on GCP.
3.5	**Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse.**	For customers using Cloud Key Management System (KMS) or Cloud Hardware Security Module (HSM), Google has PCI DSS compliance responsibility for dedicated internal Google Production and management network systems. For computer resources that are provided by Google to customers as part of a customer's GCP project, the PCI compliance of those resources is the customer's responsibility.	GCP customers are responsible for meeting the requirements of section 3 for any cardholder data transmitted to or stored within their instances, applications or databases on GCP.
3.5.1	Maintain a documented description of the cryptographic architecture that includes:	For customers using Cloud Key Management System (KMS) or Cloud	This is an additional requirement for service providers only.

	• Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date • Description of the key usage for each key. • Inventory of any HSMs and other SCDs used for key management	Hardware Security Module (HSM), Google has PCI DSS compliance responsibility for dedicated internal Google Production and management network systems. For computer resources that are provided by Google to customers as part of a customer's GCP project, the PCI compliance of those resources is the customer's responsibility.	
3.5.2	Restrict access to cryptographic keys to the fewest number of custodians necessary.	For customers using Cloud Key Management System (KMS) or Cloud Hardware Security Module (HSM), Google has PCI DSS compliance responsibility for dedicated internal Google Production and management network systems. For computer resources that are provided by Google to customers as part of a customer's GCP project, the PCI compliance of those resources is the customer's responsibility.	GCP customers are responsible for meeting the requirements of section 3 for any cardholder data transmitted to or stored within their instances, applications or databases on GCP.
3.5.3	Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times: • Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key. • Within a secure cryptographic device (such as a hardware/host security module (HSM) or PTS-approved point-of-interaction device). • As at least two full-length key components or key	It is outside the the scope of Google's PCI assessment to comply with requirements of section 3 for cardholder data stored within any customer instances on GCP. Cloud Key Management System (KMS) oe or Cloud Hardware Security Module (HSM) has PCI Compliant procedures. However customers are responsible on how to use Cloud KMS or Cloud HSM to protect cardholder data.	GCP customers are responsible for meeting the requirements of section 3 for any cardholder data transmitted to or stored within their instances, applications or databases on GCP.

	shares, in accordance with an industry-accepted method.		
3.5.4	Store cryptographic keys in the fewest possible locations.	For customers using Cloud Key Management System (KMS) or Cloud Hardware Security Module (HSM), Google has PCI DSS compliance responsibility for dedicated internal Google Production and management network systems. For computer resources that are provided by Google to customers as part of a customer's GCP project, the PCI compliance of those resources is the customer's responsibility.	GCP customers are responsible for meeting the requirements of section 3 for any cardholder data transmitted to or stored within their instances, applications or databases on GCP.
3.6	**Fully document and implement all key management processes and procedures for cryptographic keys used for encryption of cardholder data.**	The Cloud Key Management System (KMS) or Cloud Hardware Security Module (HSM) service has internal key management procedures that are validated to be PCI DSS compliant. Cloud KMS or Cloud HSM customers are responsible for how they choose to use this service to implement their own PCI compliant encryption systems. For customers who choose not to use Cloud KMS or Cloud HSM as part of their cardholder data protection, this item is fully a customer responsibility.	GCP customers are responsible for meeting the requirements of section 3 for any cardholder data transmitted to or stored within their instances, applications or databases on GCP.

3.6.1	Generation of strong cryptographic keys.	The Cloud Key Management System (KMS) or Cloud Hardware Security Module (HSM) service has internal key management procedures that are validated to be PCI DSS compliant. Cloud KMS or Cloud HSM customers are responsible for how they choose to use this service to implement their own PCI compliant encryption systems. For customers who choose not to use Cloud KMS or Cloud HSM as part of their cardholder data protection, this item is fully a customer responsibility.	GCP customers are responsible for meeting the requirements of section 3 for any cardholder data transmitted to or stored within their instances, applications or databases on GCP.
3.6.2	Secure cryptographic key distribution.	The Cloud Key Management System (KMS) or Cloud Hardware Security Module (HSM) service has internal key management procedures that are validated to be PCI DSS compliant. Cloud KMS or Cloud HSM customers are responsible for how they choose to use this service to implement their own PCI compliant encryption systems. For customers who choose not to use Cloud KMS or Cloud HSM as part of their cardholder data protection, this item is fully a customer responsibility.	GCP customers are responsible for meeting the requirements of section 3 for any cardholder data transmitted to or stored within their instances, applications or databases on GCP.

3.6.3	Secure cryptographic key storage	The Cloud Key Management System (KMS) or Cloud Hardware Security Module (HSM) service has internal key management procedures that are validated to be PCI DSS compliant. Cloud KMS or Cloud HSM customers are responsible for how they choose to use this service to implement their own PCI compliant encryption systems. For customers who choose not to use Cloud KMS or Cloud HSM as part of their cardholder data protection, this item is fully a customer responsibility.	GCP customers are responsible for meeting the requirements of section 3 for any cardholder data transmitted to or stored within their instances, applications or databases on GCP.
3.6.4	Cryptographic key changes for keys that have reached the end of their crypto-period (for example, after a defined period of time has passed and/or after a certain amount of ciphertext has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines.	The Cloud Key Management System (KMS) or Cloud Hardware Security Module (HSM) service has internal key management procedures that are validated to be PCI DSS compliant. Cloud KMS or Cloud HSM customers are responsible for how they choose to use this service to implement their own PCI compliant encryption systems. For customers who choose not to use Cloud KMS or Cloud HSM as part of their cardholder data protection, this item is fully a customer responsibility.	GCP customers are responsible for meeting the requirements of section 3 for any cardholder data transmitted to or stored within their instances, applications or databases on GCP.

3.6.5	Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear text key component), or keys are suspected of being compromised.	The Cloud Key Management System (KMS) or Cloud Hardware Security Module (HSM) service has internal key management procedures that are validated to be PCI DSS compliant. Cloud KMS or Cloud HSM customers are responsible for how they choose to use this service to implement their own PCI compliant encryption systems. For customers who choose not to use Cloud KMS or Cloud HSM as part of their cardholder data protection, this item is fully a customer responsibility.	GCP customers are responsible for meeting the requirements of section 3 for any cardholder data transmitted to or stored within their instances, applications or databases on GCP.
3.6.6	If manual clear text cryptographic key management operations are used, these operations must be managed using split knowledge and dual control. Note: Examples of manual key management operations include, but are not limited to: key generation, transmission, loading, storage and destruction.	Google does not use clear text cryptographic key management. This is a customer responsibility.	GCP customers are responsible for meeting the requirements of section 3 for any cardholder data transmitted to or stored within their instances, applications or databases on GCP.
3.6.7	Prevention of unauthorized substitution of cryptographic keys.	The Cloud Key Management System (KMS) or Cloud Hardware Security Module (HSM) service has internal key management procedures that are validated to be PCI DSS compliant. Cloud KMS or Cloud HSM customers are	GCP customers are responsible for meeting the requirements of section 3 for any cardholder data transmitted to or stored within their instances, applications or databases on GCP.

		responsible for how they choose to use this service to implement their own PCI compliant encryption systems. For customers who choose not to use Cloud KMS or Cloud HSM as part of their cardholder data protection, this item is fully a customer responsibility.	
3.6.8	Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key custodian responsibilities.	The Cloud Key Management System (KMS) or Cloud Hardware Security Module (HSM) service has internal key management procedures that are validated to be PCI DSS compliant. Cloud KMS or Cloud HSM customers are responsible for how they choose to use this service to implement their own PCI compliant encryption systems. For customers who choose not to use Cloud KMS or Cloud HSM as part of their cardholder data protection, this item is fully a customer responsibility.	GCP customers are responsible for meeting the requirements of section 3 for any cardholder data transmitted to or stored within their instances, applications or databases on GCP.
3.7	**Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties.**	The Cloud Key Management System (KMS) or Cloud Hardware Security Module (HSM) service has internal key management procedures that are validated to be PCI DSS compliant. Cloud KMS or Cloud HSM customers are	GCP customers are responsible for meeting the requirements of section 3 for any cardholder data transmitted to or stored within their instances, applications or databases on GCP.

		responsible for how they choose to use this service to implement their own PCI compliant encryption systems. For customers who choose not to use Cloud KMS or Cloud HSM as part of their cardholder data protection, this item is fully a customer responsibility.

Product Specific Customer Considerations

Product	Requirement	PCI-DSS Requirement	Additional Customer Responsibility
Stackdriver Trace	3.1	Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage: ● Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements ● Processes for secure deletion of data when no longer needed ● Specific retention requirements for cardholder data ● A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.	GCP customers are responsible for not using sensitive cardholder data while using the trace functionalities in Stackdriver Trace product.
Stackdriver Trace	3.2	Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization	GCP customers are responsible for not using sensitive cardholder data while using the trace functionalities in Stackdriver Trace product.

		process. It is permissible for issuers and companies that support issuing services to store sensitive authentication data if: There is a business justification and The data is stored securely.	
Cloud SQL	3.2	Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process. It is permissible for issuers and companies that support issuing services to store sensitive authentication data if: There is a business justification and The data is stored securely.	Encryption of cardholder data in the Cloud SQL system either at rest or in transmit is the responsibility of Cloud SQL customer.
Cloud SQL	3.4	Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: ● One way hashes based on strong cryptographic, (hash must be of the entire PAN) ● Truncation (hashing cannot be used to replace the truncated segment of PAN) ● Index tokens and pads (pads must be securely stored) ● Strong cryptography with associated key management processes and procedures.	Encryption of cardholder data in the Cloud SQL system either at rest or in transmit is the responsibility of Cloud SQL customer.
Cloud SQL **&** **Cloud Key Management System (KMS)** **OR Cloud**	3.5	Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse.	Encryption of cardholder data in the Cloud SQL system either at rest or in transmit is the responsibility of Cloud SQL customer. Customers should ensure that Cloud Key Management System (KMS) or Cloud Hardware Security Module (HSM) is configured as per the PCI DSS requirements in section 3.5

Hardware Security Module (HSM)			
Cloud SQL **&** **Cloud Key Management System (KMS)** **OR** **Cloud Hardware Security Module (HSM)**	3.6	Fully document and implement all key management processes and procedures for cryptographic keys used for encryption of cardholder data.	Encryption of cardholder data in the Cloud SQL system either at rest or in transmit is the responsibility of Cloud SQL customer. Customers should ensure that Cloud Key Management System (KMS) or Cloud Hardware Security Module (HSM) is configured as per the PCI DSS requirements in section 3.5

Product Specific Considerations for Google

Product	Requirement	PCI-DSS Requirement	Additional Google Responsibility
Transfer Appliance	3.1	Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage: ● Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements ● Processes for secure deletion of data when no longer needed ● Specific retention requirements for cardholder data	Google is responsible for ensuring that the data in the appliance is securely wiped.

	• A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention	

Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks

Requirement	Description	GCP	Customer
4.1	**Use strong cryptography and security protocols (for example, TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks, including the following:** ● **Only trusted keys and certificates are accepted** ● **The protocol in use only supports secure versions or configurations** ● **The encryption strength is appropriate for the encryption methodology in use**	Google has implemented configuration standards that comply with requirements in section 4.1 for the infrastructure underlying GCP products in scope for PCI. For all Google Cloud Service API endpoints, such as translate.googleapis.com, speech.googleapis.com, www.googleapis.com/storage and similar, customers are responsible for using web browsers and client endpoints that do not support TLS1.0 or ciphers that are weaker than AES128.	GCP customers are responsible for ensuring that appropriate security protocols, in compliance with section 4, are implemented for all transmissions of cardholder data over public networks into GCP. Customers are also responsible for any transmission of CHD over public networks that they initiate in their own software within Google Cloud Platform.
4.1.1	Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission.	Any transmission of Cardholder Data over wireless networks is Customer responsibility.	GCP customers are responsible for ensuring that appropriate security protocols, in compliance with section 4, are implemented for all transmissions of cardholder data over public networks into GCP.
4.2	**Never send unprotected PANs by end user messaging**	Google has implemented configuration	GCP customers are responsible for

	technologies (for example, email, instant messaging, chat, etc.).	standards that comply with requirements in section 4.2 for the infrastructure underlying GCP products in scope for PCI.	ensuring that appropriate security protocols, in compliance with section 4, are implemented for all transmissions of cardholder data over public networks into GCP.
4.3	**Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties.**	Google has implemented configuration standards that comply with requirements in section 4.3 for the infrastructure underlying GCP products in scope for PCI.	GCP customers are responsible for ensuring that appropriate security protocols, in compliance with section 4, are implemented for all transmissions of cardholder data over public networks into GCP.

Product Specific Customer Considerations

Product	Requirement	PCI-DSS Requirement	Additional Customer Responsibility
Cloud SQL	4.1	Use strong cryptography and security protocols (for example, TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks, including the following: ● only trusted keys and certificates are accepted. ● the protocol in use only supports secure versions or configurations. ● the encryption strength is appropriate for the encryption methodology in use.	Encryption of cardholder data in the Cloud SQL system either at rest or in transmit is the responsibility of Cloud SQL customer.

Requirement 5: Protect all Systems Against Malware and Regularly Update Anti-Virus Software or Programs

Requirement	Description	GCP	Customer
5.1	**Deploy antivirus software on all systems commonly affected by malicious software (particularly personal computers and servers).**	Google is responsible for the implementation of malware protection in the underlying GCP infrastructure in compliance with section 5 requirements. Google **is not responsible** for the implementation of malware protection within any customer deployed instances on GCP.	GCP customers are responsible for implementing malware protection on any customer deployed instances within GCP in compliance with section 5 requirements.
5.1.1	Ensure that antivirus programs are capable of detecting, removing, and protecting against all known types of malicious software.	Google is responsible for the implementation of malware protection in the underlying GCP infrastructure in compliance with section 5 requirements. Google **is not responsible** for the implementation of malware protection within any customer deployed instances on GCP.	GCP customers are responsible for implementing malware protection on any customer deployed instances within GCP in compliance with section 5 requirements.
5.1.2	For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.	Google is responsible for the implementation of malware protection in the underlying GCP infrastructure in compliance with section 5 requirements.	GCP customers are responsible for implementing malware protection on any customer deployed instances within GCP in compliance with section 5 requirements.

		Google **is not responsible** for the implementation of malware protection within any customer deployed instances on GCP.	
5.2	**Ensure that all antivirus mechanisms are maintained as follows:** ● **Are kept current** ● **Perform periodic scans** ● **Generate audit logs which are retained per PCI DSS Requirement 10.7.**	Google is responsible for the implementation of malware protection in the underlying GCP infrastructure in compliance with section 5 requirements. Google **is not responsible** for the implementation of malware protection within any customer deployed instances on GCP.	GCP customers are responsible for implementing malware protection on any customer deployed instances within GCP in compliance with section 5 requirements.
5.3	**Ensure that antivirus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.**	Google is responsible for the implementation of malware protection in the underlying GCP infrastructure in compliance with section 5 requirements. Google **is not responsible** for the implementation of malware protection within any customer deployed instances on GCP.	GCP customers are responsible for implementing malware protection on any customer deployed instances within GCP in compliance with section 5 requirements.
5.4	**Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.**	Google is responsible for the implementation of malware protection in the underlying GCP infrastructure in compliance with section 5 requirements. Google **is not responsible** for the	GCP customers are responsible for implementing malware protection on any customer deployed instances within GCP in compliance with section 5 requirements.

		implementation of malware protection within any customer deployed instances on GCP.	

Requirement 6: Develop and Maintain Secure Systems and Applications

Requirement	Description	GCP	Customer
6.1	**Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities.**	Google is responsible for protecting the systems and infrastructure underlying GCP from vulnerabilities in compliance with the requirements in section 6.	GCP customers are responsible for protecting customer deployed instances and software on GCP from vulnerabilities in compliance with section 6 requirements.
6.2	**Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor supplied security patches. Install critical security patches within one month of release.**	Google is responsible for protecting the systems and infrastructure underlying GCP from vulnerabilities in compliance with the requirements in section 6.	GCP customers are responsible for protecting customer deployed instances and software on GCP from vulnerabilities in compliance with section 6 requirements.
6.3	Develop internal and external software applications (including web based administrative access to applications) securely, as follows: ● In accordance with PCI DSS (for example, secure authentication and logging) ● Based on industry standards and/or best practices ● Incorporating information security throughout the software- development life cycle	Google is responsible for protecting the systems and infrastructure underlying GCP from vulnerabilities in compliance with the requirements in section 6.	GCP customers are responsible for protecting customer deployed instances and software on GCP from vulnerabilities in compliance with section 6 requirements.
6.3.1	Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers.	Google is responsible for protecting the systems and infrastructure underlying GCP from vulnerabilities in compliance with the requirements in section 6.	GCP customers are responsible for protecting customer deployed instances and software on GCP from vulnerabilities in compliance with section 6

			requirements.
6.3.2	Review custom code prior to release to production or customers in order to identify any potential coding vulnerability (using either manual or automated processes).	Google is responsible for protecting the systems and infrastructure underlying GCP from vulnerabilities in compliance with the requirements in section 6.	GCP customers are responsible for protecting customer deployed instances and software on GCP from vulnerabilities in compliance with section 6 requirements.
6.4	**Follow change control processes and procedures for all changes to system components. The processes must include the following:**		
6.4.1	Separate development/test environments from production environments, and enforce the separation with access controls.	Google is responsible for protecting the systems and infrastructure underlying GCP from vulnerabilities in compliance with the requirements in section 6.	GCP customers are responsible for protecting customer deployed instances and software on GCP from vulnerabilities in compliance with section 6 requirements.
6.4.2	Separation of duties between development/test and production environments.	Google is responsible for protecting the systems and infrastructure underlying GCP from vulnerabilities in compliance with the requirements in section 6.	GCP customers are responsible for protecting customer deployed instances and software on GCP from vulnerabilities in compliance with section 6 requirements.
6.4.3	Production data (live PANs) are not used for testing or development.	Google is responsible for protecting the systems and infrastructure underlying GCP from vulnerabilities in compliance with the	GCP customers are responsible for protecting customer deployed instances and software on GCP from vulnerabilities

		requirements in section 6.	in compliance with section 6 requirements.
6.4.4	Removal of test data and accounts before production systems become active.	Google is responsible for protecting the systems and infrastructure underlying GCP from vulnerabilities in compliance with the requirements in section 6.	GCP customers are responsible for protecting customer deployed instances and software on GCP from vulnerabilities in compliance with section 6 requirements.
6.4.5	Change control procedures for the implementation of security patches and software modifications must include the following:		
6.4.5.1	Documentation of impact.	Google is responsible for protecting the systems and infrastructure underlying GCP from vulnerabilities in compliance with the requirements in section 6.	GCP customers are responsible for protecting customer deployed instances and software on GCP from vulnerabilities in compliance with section 6 requirements.
6.4.5.2	Documented change approval by authorized parties.	Google is responsible for protecting the systems and infrastructure underlying GCP from vulnerabilities in compliance with the requirements in section 6.	GCP customers are responsible for protecting customer deployed instances and software on GCP from vulnerabilities in compliance with section 6 requirements.
6.4.5.3	Functionality testing to verify that the change does not adversely impact the security of the system.	Google is responsible for protecting the systems and infrastructure underlying GCP	GCP customers are responsible for protecting customer deployed instances

		from vulnerabilities in compliance with the requirements in section 6.	and software on GCP from vulnerabilities in compliance with section 6 requirements.
6.4.5.4	Back-out procedures.	Google is responsible for protecting the systems and infrastructure underlying GCP from vulnerabilities in compliance with the requirements in section 6.	GCP customers are responsible for protecting customer deployed instances and software on GCP from vulnerabilities in compliance with section 6 requirements.
6.4.6	Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable.	Google has PCI DSS compliance responsibility for dedicated internal Google Production and management network systems.	For computer resources that are provided by Google to customers as part of a customer's GCP project, the PCI compliance of those resources is the customer's responsibility.
6.5	**Address common coding vulnerabilities in software-development processes as follows:** ● **Train developers in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory.** ● **Develop applications based on secure coding** guidelines.	Google is responsible for protecting the systems and infrastructure underlying GCP from vulnerabilities in compliance with the requirements in section 6.	GCP customers are responsible for protecting customer deployed instances and software on GCP from vulnerabilities in compliance with section 6 requirements.
6.5.1	Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.	Google is responsible for protecting the systems and infrastructure underlying GCP from vulnerabilities in compliance with the	GCP customers are responsible for protecting customer deployed instances and software on GCP from vulnerabilities

		requirements in section 6.	in compliance with section 6 requirements.
6.5.2	Buffer overflows.	Google is responsible for protecting the systems and infrastructure underlying GCP from vulnerabilities in compliance with the requirements in section 6.	GCP customers are responsible for protecting customer deployed instances and software on GCP from vulnerabilities in compliance with section 6 requirements.
6.5.3	Insecure cryptographic storage.	Google is responsible for protecting the systems and infrastructure underlying GCP from vulnerabilities in compliance with the requirements in section 6.	GCP customers are responsible for protecting customer deployed instances and software on GCP from vulnerabilities in compliance with section 6 requirements.
6.5.4	Insecure communications.	Google is responsible for protecting the systems and infrastructure underlying GCP from vulnerabilities in compliance with the requirements in section 6.	GCP customers are responsible for protecting customer deployed instances and software on GCP from vulnerabilities in compliance with section 6 requirements.
6.5.5	Improper error handling.	Google is responsible for protecting the systems and infrastructure underlying GCP from vulnerabilities in compliance with the requirements in section 6.	GCP customers are responsible for protecting customer deployed instances and software on GCP from vulnerabilities in compliance with section 6 requirements.

6.5.6	All “high risk” vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1).	Google is responsible for protecting the systems and infrastructure underlying GCP from vulnerabilities in compliance with the requirements in section 6.	GCP customers are responsible for protecting customer deployed instances and software on GCP from vulnerabilities in compliance with section 6 requirements.
6.5.7	Cross-site scripting (XSS).	Google is responsible for protecting the systems and infrastructure underlying GCP from vulnerabilities in compliance with the requirements in section 6.	GCP customers are responsible for protecting customer deployed instances and software on GCP from vulnerabilities in compliance with section 6 requirements.
6.5.8	Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions).	Google is responsible for protecting the systems and infrastructure underlying GCP from vulnerabilities in compliance with the requirements in section 6.	GCP customers are responsible for protecting customer deployed instances and software on GCP from vulnerabilities in compliance with section 6 requirements.
6.5.9	Cross-site request forgery (CSRF).	Google is responsible for protecting the systems and infrastructure underlying GCP from vulnerabilities in compliance with the requirements in section 6.	GCP customers are responsible for protecting customer deployed instances and software on GCP from vulnerabilities in compliance with section 6 requirements.
6.5.10	Broken authentication and session management Note: Requirement 6.5.10 is a best practice until June 30, 2015, after which it becomes a requirement.	Google is responsible for protecting the systems and infrastructure underlying GCP from vulnerabilities in compliance with the requirements in section 6.	GCP customers are responsible for protecting customer deployed instances and software on GCP from vulnerabilities in compliance with section 6 requirements.

6.6	**For public facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods:** ● **Reviewing public facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes (Note: This assessment is not the same as the vulnerability scans performed for Requirement 11.2)** ● **Installing an automated technical solution that detects and prevents web based attacks (for example, a web application firewall) in front of public facing web applications, to continually check all traffic**	Google is responsible for protecting the systems and infrastructure underlying GCP from vulnerabilities in compliance with the requirements in section 6.	GCP customers are responsible for protecting customer deployed instances and software on GCP from vulnerabilities in compliance with section 6 requirements.
6.7	**Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties.**	Google is responsible for protecting the systems and infrastructure underlying GCP from vulnerabilities in compliance with the requirements in section 6.	GCP customers are responsible for protecting customer deployed instances and software on GCP from vulnerabilities in compliance with section 6 requirements.

Product Specific Customer Considerations

Product	Requirement	PCI-DSS Requirement	Additional Customer Responsibility

Cloud Dataproc	6.3 6.3.1 6.3.2	Develop internal and external software applications (including web based administrative access to applications) securely, as follows: ● in accordance with PCI DSS (for example, secure authentication and logging) ● based on industry standards and/or best practices ● incorporating information security throughout the software- development life cycle	Customers are responsible for re-imaging their environments.
Container Engine	6.3 6.3.1 6.3.2	Develop internal and external software applications (including web based administrative access to applications) securely, as follows: ● in accordance with PCI DSS (for example, secure authentication and logging) ● based on industry standards and/or best practices ● incorporating information security throughout the software- development life cycle	Customers should use only pre-built images (Container-Optimized Google Compute Engine Images)
Container Builder	6.4 6.4.1 6.4.2 6.4.3 6.4.4 6.4.5 6.4.6	Follow change control processes and procedures for all changes to system components.	GCP customers are responsible for all updated (i.e. non Google pre-built) GCP instances being used.

Requirement 7: Restrict Access to Cardholders Data by Business Need to Know

Requirement	Description	GCP	Customer
7.1	**Limit access to system components and cardholder data to only those individuals whose job requires such access.**	Google is responsible for implementing access controls in compliance with the requirements of sections 7 and 8 for the systems and infrastructure underlying GCP.	GCP customers are responsible for implementing access controls on customer instances and applications in compliance with the requirements of sections 7 and 8.
7.1.1	Define access needs for each role, including: ● System components and data resources that each role needs to access for their job function ● Level of privilege required (for example, user, administrator, etc.) for accessing resources.	Google is responsible for implementing access controls in compliance with the requirements of sections 7 and 8 for the systems and infrastructure underlying GCP.	GCP customers are responsible for implementing access controls on customer instances and applications in compliance with the requirements of sections 7 and 8.
7.1.2	Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.	Google is responsible for implementing access controls in compliance with the requirements of sections 7 and 8 for the systems and infrastructure underlying GCP.	GCP customers are responsible for implementing access controls on customer instances and applications in compliance with the requirements of sections 7 and 8.
7.1.3	Assign access based on individual personnel's job classification and function.	Google is responsible for implementing access controls in compliance with the requirements of sections 7 and 8 for the systems and infrastructure underlying GCP.	GCP customers are responsible for implementing access controls on customer instances and applications in compliance with the requirements of sections 7 and 8.

7.1.4	Require documented approval by authorized parties specifying required privileges.	Google is responsible for implementing access controls in compliance with the requirements of sections 7 and 8 for the systems and infrastructure underlying GCP.	GCP customers are responsible for implementing access controls on customer instances and applications in compliance with the requirements of sections 7 and 8.
7.2	**Establish an access control system for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system must include the following:**	**Google is responsible for implementing access controls in compliance with the requirements of sections 7 and 8 for the systems and infrastructure underlying GCP.**	**GCP customers are responsible for implementing access controls on customer instances and applications in compliance with the requirements of sections 7 and 8.**
7.2.1	Coverage of all system components.	Google is responsible for implementing access controls in compliance with the requirements of sections 7 and 8 for the systems and infrastructure underlying GCP.	GCP customers are responsible for implementing access controls on customer instances and applications in compliance with the requirements of sections 7 and 8.
7.2.2	Assignment of privileges to individuals based on job classification and function.	Google is responsible for implementing access controls in compliance with the requirements of sections 7 and 8 for the systems and infrastructure underlying GCP.	GCP customers are responsible for implementing access controls on customer instances and applications in compliance with the requirements of sections 7 and 8.
7.2.3	Default "deny all" setting.	Google is responsible for implementing access controls in compliance with the requirements of sections 7 and 8 for the systems and infrastructure underlying GCP.	GCP customers are responsible for implementing access controls on customer instances and applications in compliance with the requirements of sections 7 and 8.

7.3	**Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.**	**Google is responsible for implementing access controls in compliance with the requirements of sections 7 and 8 for the systems and infrastructure underlying GCP.**	**GCP customers are responsible for implementing access controls on customer instances and applications in compliance with the requirements of sections 7 and 8.**

Product Specific Customer Considerations

Product	Requirement	PCI-DSS Requirement	Additional Customer Responsibility
Cloud SQL	7.1	Limit access to system components and cardholder data to only those individuals whose job requires such access.	Cloud SQL customers are responsible for mySQL user access management.
Cloud SQL	7.3	Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.	Cloud SQL customers are responsible for mySQL user access management.

Requirement 8: Identify and Authenticate Access to System Components

Requirement	Description	GCP	Customer
8.1	**Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows:**	**Google is responsible for implementing access controls in compliance with the requirements of sections 7 and 8 for the systems and infrastructure underlying GCP.**	**GCP customers are responsible for implementing access controls on customer instances and applications in compliance with the requirements of sections 7 and 8.**
8.1.1	Assign all users a unique ID before allowing them to access system components or cardholder data.	Google is responsible for implementing access controls in compliance with the requirements of sections 7 and 8 for the systems and infrastructure underlying GCP.	GCP customers are responsible for implementing access controls on customer instances and applications in compliance with the requirements of sections 7 and 8.
8.1.2	Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	Google is responsible for implementing access controls in compliance with the requirements of sections 7 and 8 for the systems and infrastructure underlying GCP.	GCP customers are responsible for implementing access controls on customer instances and applications in compliance with the requirements of sections 7 and 8.
8.1.3	Immediately revoke access for any terminated users.	Google is responsible for implementing access controls in compliance with the requirements of sections 7 and 8 for the systems and infrastructure underlying GCP.	GCP customers are responsible for implementing access controls on customer instances and applications in compliance with the requirements of sections 7 and 8.

8.1.4	Remove/disable inactive user accounts at least every 90 days.	Google is responsible for implementing access controls in compliance with the requirements of sections 7 and 8 for the systems and infrastructure underlying GCP.	GCP customers are responsible for implementing access controls on customer instances and applications in compliance with the requirements of sections 7 and 8.
8.1.5	Manage IDs used by vendors to access, support, or maintain system components via remote access as follows: ● Enabled only during the time period needed and disabled when not in use. ● Monitored when in use.	Google is responsible for implementing access controls in compliance with the requirements of sections 7 and 8 for the systems and infrastructure underlying GCP.	GCP customers are responsible for implementing access controls on customer instances and applications in compliance with the requirements of sections 7 and 8.
8.1.6	Limit repeated access attempts by locking out the user ID after not more than six attempts.	Google is responsible for implementing access controls in compliance with the requirements of sections 7 and 8 for the systems and infrastructure underlying GCP. Additionally, Google is responsible for reviewing internal processes and customer/user documentation, and observing implemented processes to verify that non-consumer customer user accounts are temporarily locked-out after not more than six invalid access attempts. 8.1.6.b is a customer responsibility.	GCP customers are responsible for implementing access controls on customer instances and applications in compliance with the requirements of sections 7 and 8.
8.1.7	Set the lockout duration to a minimum of 30 minutes or until	Google is responsible for implementing	GCP customers are responsible for

	an administrator enables the user ID.	access controls in compliance with the requirements of sections 7 and 8 for the systems and infrastructure underlying GCP.	implementing access controls on customer instances and applications in compliance with the requirements of sections 7 and 8.
8.1.8	If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	Google is responsible for implementing access controls in compliance with the requirements of sections 7 and 8 for the systems and infrastructure underlying GCP.	GCP customers are responsible for implementing access controls on customer instances and applications in compliance with the requirements of sections 7 and 8.
8.2	**In addition to assigning a unique ID, ensure proper user authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users:** ● **Something you know, such as a password or passphrase.** ● **Something you have, such as a token device or smart card.** ● **Something you are, such as a biometric.**	Google is responsible for implementing access controls in compliance with the requirements of sections 7 and 8 for the systems and infrastructure underlying GCP.	GCP customers are responsible for implementing access controls on customer instances and applications in compliance with the requirements of sections 7 and 8.
8.2.1	Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.	Google is responsible for implementing access controls in compliance with the requirements of sections 7 and 8 for the systems and infrastructure underlying GCP.	GCP customers are responsible for implementing access controls on customer instances and applications in compliance with the requirements of sections 7 and 8.

8.2.2	Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys.	Google is responsible for implementing access controls in compliance with the requirements of sections 7 and 8 for the systems and infrastructure underlying GCP.	GCP customers are responsible for implementing access controls on customer instances and applications in compliance with the requirements of sections 7 and 8.
8.2.3	Passwords/phrases must meet the following: ● Require a minimum length of at least seven characters. ● Contain both numeric and alphabetic characters. ● Alternatively, the passwords/phrases must have complexity and strength at least equivalent to the parameters specified above.	Google is responsible for implementing access controls in compliance with the requirements of sections 7 and 8 for the systems and infrastructure underlying GCP. 8.2.3.b is customer responsibility	GCP customers are responsible for implementing access controls on customer instances and applications in compliance with the requirements of sections 7 and 8.
8.2.4	Change user passwords/passphrases at least every 90 days.	Google is responsible for implementing access controls in compliance with the requirements of sections 7 and 8 for the systems and infrastructure underlying GCP. 8.2.4.b is customer responsibility.	GCP customers are responsible for implementing access controls on customer instances and applications in compliance with the requirements of sections 7 and 8.
8.2.5	Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used.	Google is responsible for implementing access controls in compliance with the requirements of sections 7 and 8 for the systems and infrastructure underlying GCP. 8.2.5.b is customer responsibility.	GCP customers are responsible for implementing access controls on customer instances and applications in compliance with the requirements of sections 7 and 8.

8.2.6	Set passwords/phrases for first time use and upon reset to a unique value for each user, and change immediately after the first use.	Google is responsible for implementing access controls in compliance with the requirements of sections 7 and 8 for the systems and infrastructure underlying GCP.	GCP customers are responsible for implementing access controls on customer instances and applications in compliance with the requirements of sections 7 and 8.
8.3	**Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication.**	Google is responsible for implementing access controls in compliance with the requirements of sections 7 and 8 for the systems and infrastructure underlying GCP.	GCP customers are responsible for implementing access controls on customer instances and applications in compliance with the requirements of sections 7 and 8.
8.3.1	Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.	Google is responsible for implementing access controls in compliance with the requirements of sections 7 and 8 for the systems and infrastructure underlying GCP.	GCP customers are responsible for implementing access controls on customer instances and applications in compliance with the requirements of sections 7 and 8.
8.3.2	Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third party access for support or maintenance) originating from outside the entity's network.	Google is responsible for implementing access controls in compliance with the requirements of sections 7 and 8 for the systems and infrastructure underlying GCP.	GCP customers are responsible for implementing access controls on customer instances and applications in compliance with the requirements of sections 7 and 8.
8.4	**Document and communicate authentication procedures and policies to all users including:** ● **Guidance on selecting strong authentication**	Google is responsible for implementing access controls in compliance with the requirements of sections 7 and 8 for the	GCP customers are responsible for implementing access controls on customer instances and applications in

	credentials. • **Guidance for how users should protect their authentication credentials.** • **Instructions not to reuse previously used passwords.** • **Instructions to change passwords if there is any suspicion the password could be compromised.**	systems and infrastructure underlying GCP.	compliance with the requirements of sections 7 and 8.
8.5	**Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows:** • **Generic user IDs are disabled or removed** • **Shared user IDs do not exist for system administration and other critical functions** • **Shared and generic user IDs are not used to administer any system components**	Google is responsible for implementing access controls in compliance with the requirements of sections 7 and 8 for the systems and infrastructure underlying GCP.	GCP customers are responsible for implementing access controls on customer instances and applications in compliance with the requirements of sections 7 and 8.
8.5.1	Additional requirement for service providers: Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer.	Google does not have remote access to its customer's premises.	GCP customers are responsible for implementing access controls on customer instances and applications in compliance with the requirements of sections 7 and 8.
8.6	**Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows:** • **Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts.** • **Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.**	Google is responsible for implementing access controls in compliance with the requirements of sections 7 and 8 for the systems and infrastructure underlying GCP.	GCP customers are responsible for implementing access controls on customer instances and applications in compliance with the requirements of sections 7 and 8.

8.7	**All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows:** • **All user access to, user queries of, and user actions on databases are through programmatic methods.** • **Only database administrators have the ability to directly access or query databases.** • **Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).**	Google is responsible for implementing access controls in compliance with the requirements of sections 7 and 8 for the systems and infrastructure underlying GCP.	GCP customers are responsible for implementing access controls on customer instances and applications in compliance with the requirements of sections 7 and 8. Database administration is customer responsibility.
8.8	**Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.**	Google is responsible for implementing access controls in compliance with the requirements of sections 7 and 8 for the systems and infrastructure underlying GCP.	GCP customers are responsible for implementing access controls on customer instances and applications in compliance with the requirements of sections 7 and 8.

Product Specific Customer Considerations

Product	Requirement	PCI-DSS Requirement	Additional Customer Responsibility
Deployment Manager	8.1	Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components.	Customers are responsible for management (including revocation, termination, suspension etc.) of generic / robot accounts.
Cloud SQL	8.1	Define and implement policies and procedures to ensure proper	Cloud SQL customers are responsible for

		user identification management for non-consumer users and administrators on all system components.	mySQL user access management.
Cloud SQL	8.3	Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication.	Cloud SQL customers are responsible for mySQL user access management.
Cloud SQL	8.6	Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows: ● authentication mechanisms must be assigned to an individual account and not shared among multiple accounts. ● physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.	Cloud SQL customers are responsible for mySQL user access management.
Transfer Appliance	8.6	Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows: ● authentication mechanisms must be assigned to an individual account and not shared among multiple accounts. ● physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.	GCP Customers are responsible for safeguarding the passphrase that generates the temporary encryption key in the appliance to encrypt the data and decryption key to decrypt data in the GCP final bucket
Cloud SQL	8.7	All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows:	Cloud SQL customers are responsible for mySQL user access management.

		• all user access to, user queries of, and user actions on databases are through programmatic methods. • only database administrators have the ability to directly access or query databases. • application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).	

Requirement 9: Restrict Physical Access to Cardholder Data

Requirement	Description	GCP	Customer
9.1	**Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.**	Google is responsible for physical security controls on all Google Data centers underlying GCP.	N/A
9.1.1	Use video cameras and/or access control mechanisms to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law. Note: “Sensitive areas” refers to any data center, server room or any area that houses systems that store, process, or transmit cardholder data. This excludes public-facing areas where only point-of-sale terminals are present, such as the cashier areas in a retail store.	Google is responsible for physical security controls on all Google Data centers underlying GCP.	N/A

9.1.2	Implement physical and/or logical controls to restrict access to publicly accessible network jacks.	Google is responsible for physical security controls on all Google Data centers underlying GCP.	N/A
9.1.3	Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.	Google is responsible for physical security controls on all Google Data centers underlying GCP.	N/A
9.2	**Develop procedures to easily distinguish between onsite personnel and visitors, to include:** ● **Identifying new onsite personnel or visitors (for example, assigning badges).** ● **Changes to access requirements.** ● **Revoking or terminating onsite personnel and expired visitor identification (such as ID badges).**	Google is responsible for physical security controls on all Google Data centers underlying GCP.	N/A
9.3	**Control physical access for onsite personnel to the sensitive areas as follows:** ● **Access must be authorized and based on individual job function.** ● **Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled.**	Google is responsible for physical security controls on all Google Data centers underlying GCP.	N/A
9.4	**Implement procedures to identify and authorize visitors. Procedures should include the following:**	Google is responsible for physical security controls on all Google Data centers underlying GCP.	N/A

9.4.1	Visitors are authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained.	Google is responsible for physical security controls on all Google Data centers underlying GCP.	N/A
9.4.2	Visitors are identified and given a badge or other identification that expires and that visibly distinguishes the visitors from onsite personnel.	Google is responsible for physical security controls on all Google Data centers underlying GCP.	N/A
9.4.3	Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration.	Google is responsible for physical security controls on all Google Data centers underlying GCP.	N/A
9.4.4	A visitor log is used to maintain a physical audit trail of visitor activity to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted. Document the visitor's name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.	Google is responsible for physical security controls on all Google Data centers underlying GCP.	N/A
9.5	**Physically secure all media.**	Google is responsible for physical security controls on all Google Data centers underlying GCP, in addition to any backups that are performed and maintained by Google.	GCP customers are responsible for the security of any backups that are stored outside of GCP.

9.5.1	Store media backups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Review the location's security at least annually.	Google is responsible for physical security controls on all Google Data centers underlying GCP, in addition to any backups that are performed and maintained by Google.	GCP customers are responsible for the security of any backups that are stored outside of GCP.
9.6	**Maintain strict control over the internal or external distribution of any kind of media, including the following:**	Google is responsible for physical security controls on all Google Data centers underlying GCP, in addition to any backups that are performed and maintained by Google.	GCP customers are responsible for the security of any backups that are stored outside of GCP.
9.6.1	Classify media so the sensitivity of the data can be determined.	Google is responsible for physical security controls on all Google Data centers underlying GCP, in addition to any backups that are performed and maintained by Google.	GCP customers are responsible for the security of any backups that are stored outside of GCP.
9.6.2	Send the media by secured courier or other delivery method that can be accurately tracked.	Google is responsible for physical security controls on all Google Data centers underlying GCP, in addition to any backups that are performed and maintained by Google.	GCP customers are responsible for the security of any backups that are stored outside of GCP.
9.6.3	Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals).	Google is responsible for physical security controls on all Google Data centers underlying GCP, in addition to any backups that are performed and maintained by Google.	GCP customers are responsible for the security of any backups that are stored outside of GCP.

9.7	Maintain strict control over the storage and accessibility of media.	Google is responsible for physical security controls on all Google Data centers underlying GCP, in addition to any backups that are performed and maintained by Google.	GCP customers are responsible for the security of any backups that are stored outside of GCP.
9.7.1	Properly maintain inventory logs of all media and conduct media inventories at least annually.	Google is responsible for physical security controls on all Google Data centers underlying GCP, in addition to any backups that are performed and maintained by Google.	GCP customers are responsible for the security of any backups that are stored outside of GCP.
9.8	**Destroy media when it is no longer needed for business or legal reasons as follows:**	Google is responsible for physical security controls on all Google Data centers underlying GCP, in addition to any backups that are performed and maintained by Google.	GCP customers are responsible for the security of any backups that are stored outside of GCP.
9.8.1	Shred, incinerate, or pulp hard- copy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed.	Google is responsible for physical security controls on all Google Data centers underlying GCP, in addition to any backups that are performed and maintained by Google.	GCP customers are responsible for the security of any backups that are stored outside of GCP.
9.8.2	Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.	Google is responsible for physical security controls on all Google Data centers underlying GCP, in addition to any backups	GCP customers are responsible for the security of any backups that are stored outside of GCP.

		that are performed and maintained by Google.	
9.9	**Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution.**	Google is responsible for physical security controls on all Google Data centers underlying GCP.	Google Cloud Platform has no POS devices. Any POS devices that the customer integrates with GCP are customer responsibility.
9.9.1	Maintain an up-to-date list of devices. The list should include the following: ● Make, model of device. ● Location of device (for example, the address of the site or facility where the device is located). ● Device serial number or other method of unique identification.	Google is responsible for physical security controls on all Google Data centers underlying GCP.	Google Cloud Platform has no POS devices. Any POS devices that the customer integrates with GCP are customer responsibility.
9.9.2	Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device).	Google is responsible for physical security controls on all Google Data centers underlying GCP.	Google Cloud Platform has no POS devices. Any POS devices that the customer integrates with GCP are customer responsibility.
9.9.3	Provide training for personnel to be aware of attempted tampering or replacement of devices.	Google does not provide POS POI terminals as part of its GCP infrastructure.	Google Cloud Platform has no POS devices. Any POS devices that the customer integrates with GCP are customer responsibility.

9.10	**Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties.**	Google is responsible for physical security controls on all Google Data centers underlying GCP.	GCP customers are responsible for developing and maintaining security policies and operational procedures to comply with this requirement.

Product Specific Customer Considerations

Product	Requirement	PCI-DSS Requirement	Additional Customer Responsibility
Cloud Interconnect	9.1.2	Implement physical and/or logical controls to restrict access to publicly accessible network jacks.	GCP Customers are responsible for physical and logical controls for their own, non-GCP, network and/or colocation facilities.
	9.1.3	Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.	GCP Customers are responsible for physical security controls on all network devices in on-premise and/ or colocation facilities.
Transfer Appliance	9.9.3	Provide training for personnel to be aware of attempted tampering or replacement of devices.	GCP Customers are responsible for ensuring tamper-evident seal is intact on the device when they receive the appliance and ship it back to Google. GCP Customer should reach out to Google at data-support@google.com if there is anything wrong with the shipment.

9.5	Physically secure all media.	GCP Customers are responsible for meeting the physical security requirements of Section 9 while the devices are in their care.

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Requirement	Description	GCP	Customer
10.1	**Implement audit trails to link all access to system components to each individual user.**	Google has PCI DSS compliance responsibility for dedicated internal Google Production and management network systems.	For computer resources that are provided by Google to customers as part of a customer's GCP project, the PCI compliance of those resources is the customer's responsibility.
10.2	**Implement automated audit trails for all system components to reconstruct the following events:**		
10.2.1	All individual user accesses to cardholder data.	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with the requirements of section 10.	GCP customers are responsible for controlling access, logging and monitoring on all customer deployed instances on GCP in compliance with the requirements of section 10.
10.2.2	All actions taken by any individual with root or administrative privileges.	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with the requirements of section 10.	GCP customers are responsible for controlling access, logging and monitoring on all customer deployed instances on GCP in compliance with the requirements of section 10.
10.2.3	Access to all audit trails.	Google is responsible for controlling	GCP customers are responsible for

		access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with the requirements of section 10.	controlling access, logging and monitoring on all customer deployed instances on GCP in compliance with the requirements of section 10.
10.2.4	Invalid logical access attempts.	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with the requirements of section 10.	GCP customers are responsible for controlling access, logging and monitoring on all customer deployed instances on GCP in compliance with the requirements of section 10.
10.2.5	Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges.	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with the requirements of section 10.	GCP customers are responsible for controlling access, logging and monitoring on all customer deployed instances on GCP in compliance with the requirements of section 10.
10.2.6	Initialization, stopping, or pausing of the audit logs.	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with the requirements of section 10.	GCP customers are responsible for controlling access, logging and monitoring on all customer deployed instances on GCP in compliance with the requirements of section 10.
10.2.7	Creation and deletion of system-level objects.	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with the requirements of section 10.	GCP customers are responsible for controlling access, logging and monitoring on all customer deployed instances on GCP in compliance with the requirements of section 10.

10.3	**Record at least the following audit trail entries for all system components for each event:**		
10.3.1	User identification.	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with the requirements of section 10.	GCP customers are responsible for controlling access, logging and monitoring on all customer deployed instances on GCP in compliance with the requirements of section 10.
10.3.2	Type of event.	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with the requirements of section 10.	GCP customers are responsible for controlling access, logging and monitoring on all customer deployed instances on GCP in compliance with the requirements of section 10.
10.3.3	Date and time.	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with the requirements of section 10.	GCP customers are responsible for controlling access, logging and monitoring on all customer deployed instances on GCP in compliance with the requirements of section 10.
10.3.4	Success or failure indication.	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with the requirements of	GCP customers are responsible for controlling access, logging and monitoring on all customer deployed instances on GCP in compliance with the requirements

		section 10.	of section 10.
10.3.5	Origination of event.	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with the requirements of section 10.	GCP customers are responsible for controlling access, logging and monitoring on all customer deployed instances on GCP in compliance with the requirements of section 10.
10.3.6	Identity or name of affected data, system component, or resource.	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with the requirements of section 10.	GCP customers are responsible for controlling access, logging and monitoring on all customer deployed instances on GCP in compliance with the requirements of section 10.
10.4	**Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.**	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with the requirements of section 10.	GCP customers are responsible for controlling access, logging and monitoring on all customer deployed instances on GCP in compliance with the requirements of section 10.
10.4.1	Critical systems have the correct and consistent time.	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with the requirements of section 10.	GCP customers are responsible for controlling access, logging and monitoring on all customer deployed instances on GCP in compliance with the requirements of section 10.
10.4.2	Time data is protected.	Google is responsible for controlling	GCP customers are responsible for

		access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with the requirements of section 10.	controlling access, logging and monitoring on all customer deployed instances on GCP in compliance with the requirements of section 10.
10.4.3	Time settings are received from industry accepted time sources.	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with the requirements of section 10.	GCP customers are responsible for controlling access, logging and monitoring on all customer deployed instances on GCP in compliance with the requirements of section 10.
10.5	**Secure audit trails so they cannot be altered.**	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with the requirements of section 10.	GCP customers are responsible for controlling access, logging and monitoring on all customer deployed instances on GCP in compliance with the requirements of section 10.
10.5.1	Limit viewing of audit trails to those with a job-related need.	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with the requirements of section 10.	GCP customers are responsible for controlling access, logging and monitoring on all customer deployed instances on GCP in compliance with the requirements of section 10.
10.5.2	Protect audit trail files from unauthorized modifications.	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with the requirements of section 10.	GCP customers are responsible for controlling access, logging and monitoring on all customer deployed instances on GCP in compliance with the requirements of section 10.

10.5.3	Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with the requirements of section 10.	GCP customers are responsible for controlling access, logging and monitoring on all customer deployed instances on GCP in compliance with the requirements of section 10.
10.5.4	Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with the requirements of section 10.	GCP customers are responsible for controlling access, logging and monitoring on all customer deployed instances on GCP in compliance with the requirements of section 10.
10.5.5	Use file integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with the requirements of section 10.	GCP customers are responsible for controlling access, logging and monitoring on all customer deployed instances on GCP in compliance with the requirements of section 10.
10.6	**Review logs and security events for all system components to identify anomalies or suspicious activity.** Note: Log harvesting, parsing, and alerting tools may be used to meet this Requirement.	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with the requirements of section 10.	GCP customers are responsible for controlling access, logging and monitoring on all customer deployed instances on GCP in compliance with the requirements of section 10.
10.6.1	Review the following at least daily: ● All security events. ● Logs of all system components that store, process,	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP	GCP customers are responsible for controlling access, logging and monitoring on all customer deployed instances on

	or transmit CHD and/or SAD, or that could impact the security of CHD and/or SAD. • Logs of all critical system components. • Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS) authentication servers, e-commerce redirection servers, etc.).	in compliance with the requirements of section 10.	GCP in compliance with the requirements of section 10.
10.6.2	Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment.	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with the requirements of section 10.	GCP customers are responsible for controlling access, logging and monitoring on all customer deployed instances on GCP in compliance with the requirements of section 10.
10.6.3	Follow up exceptions and anomalies identified during the review process.	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with the requirements of section 10.	GCP customers are responsible for controlling access, logging and monitoring on all customer deployed instances on GCP in compliance with the requirements of section 10.
10.7	**Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).**	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with the requirements of section 10.	GCP customers are responsible for controlling access, logging and monitoring on all customer deployed instances on GCP in compliance with the requirements of section 10.

10.8	**Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of:** • **Firewalls** • **IDS/IPS** • **FIM** • **Anti-virus** • **Physical access controls** • **Logical access controls** • **Audit logging mechanisms** • **Segmentation controls (if used)**	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with the requirements of section 10.	GCP customers are responsible for controlling access, logging and monitoring on all customer deployed instances on GCP in compliance with the requirements of section 10.
10.8.1	Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include: • Restoring security functions . • Identifying and documenting the duration (date and time start to end) of the security failure . • Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause . • Identifying and addressing any security issues that arose during the failure • Performing a risk assessment to determine whether further actions are required as a result of the security failure . • Implementing controls to prevent cause of failure from reoccurring . • Resuming monitoring of security controls .	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with the requirements of section 10.	GCP customers are responsible for controlling access, logging and monitoring on all customer deployed instances on GCP in compliance with the requirements of section 10.
10.9	**Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected**	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP	GCP customers are responsible for controlling access, logging and monitoring on all customer deployed instances on

parties.	in compliance with the requirements of section 10.	GCP in compliance with the requirements of section 10.

Product Specific Customer Considerations

Product	Requirement	PCI-DSS Requirement	Additional Customer Responsibility
Cloud SQL	10.2	Implement automated audit trails for all system components to reconstruct the following events: ● 10.2.1 : All individual user accesses to cardholder data. ● 10.2.3 : Access to all audit trails ● 10.2.4 : Invalid logical access attempts	Cloud SQL customers are responsible for mySQL user access management.
Stackdriver Logging	10.3	Record at least the following audit trail entries for all system components for each event: ● 10.3.3 - Date and time	Customers are required to manage date/time stamp and network time synchronization for the Stackdriver Logging instances used.
Stackdriver Logging	10.7	Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).	Customers are required to ensure audit log retention period for 365 days or more (with a minimum of three months immediately available online) in accordance with their policies.

Requirement 11: Regularly Test Security Systems and Processes

Requirement	Description	GCP	Customer
11.1	**Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis.**	Google is responsible for checking for the presence of unauthorized wireless access points and similar technologies within its own physical environment and in scope networks.	GCP customers are responsible for checking for the presence of unauthorized wireless access points and similar technologies within the customer's own physical environment and in scope networks.
11.1.1	Maintain an inventory of authorized wireless access points including a documented business justification.	Google is responsible for checking for the presence of unauthorized wireless access points and similar technologies within its own physical environment and in scope networks.	GCP customers are responsible for checking for the presence of unauthorized wireless access points and similar technologies within the customer's own physical environment and in scope networks
11.1.2	Implement incident response procedures in the event unauthorized wireless access points are detected.	Google is responsible for its own incident response procedures for its environment.	GCP customers are responsible for their own incident response procedures.
11.2	**Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).**	Google has PCI DSS compliance responsibility for dedicated internal Google Production and management network systems. Google is also responsible for scanning of Google managed API endpoints and Cloud Load Balancer IP addresses.	For computer resources that are provided by Google to customers as part of a customer's GCP project, the PCI compliance of those resources is the customer's responsibility. External IP addresses assigned to customer virtual machines are the

			customer's responsibility for vulnerability scanning, irrespective of whether those systems serve content through a Google managed IP address through Cloud Load Balancer.
11.2.1	Perform quarterly internal vulnerability scans and rescans as needed, until all "high-risk" vulnerabilities (as identified in Requirement 6.1) are resolved. Scans must be performed by qualified personnel.	Google is responsible for vulnerability scans, penetration tests and testing for unauthorized wireless access points on the systems and infrastructure underlying GCP in compliance with the requirements of section 11.	GCP customers are responsible for performing vulnerability scans and penetration tests on customer deployed instances on GCP in compliance with the requirements of section 11.
11.2.2	Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved.	Google is responsible for vulnerability scans, penetration tests and testing for unauthorized wireless access points on the systems and infrastructure underlying GCP in compliance with the requirements of section 11. Google is also responsible for scanning of Google managed API endpoints and Cloud Load Balancer IP addresses.	GCP customers are responsible for performing vulnerability scans and penetration tests on customer deployed instances on GCP in compliance with the requirements of section 11. External IP addresses assigned to customer virtual machines are the customer's responsibility for vulnerability scanning irrespective of whether those systems serve content through a Google managed IP address through Cloud Load Balancer.
11.2.3	Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel.	Google is responsible for vulnerability scans, penetration tests and testing for unauthorized wireless access points on the systems and infrastructure underlying	GCP customers are responsible for performing vulnerability scans and penetration tests on customer deployed instances on GCP in compliance with the

		GCP in compliance with the requirements of section 11.	requirements of section 11.
11.3	**Implement a methodology for penetration testing that includes the following:** ● **Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115).** ● **Includes coverage for the entire CDE perimeter and critical systems.** ● **Includes testing from both inside and outside the network.** ● **Includes testing to validate any segmentation and scope-reduction controls.** ● **Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5.** ● **Defines network-layer penetration tests to include components that support network functions as well as operating systems.** ● **Includes review and consideration of threats and vulnerabilities experienced in the last 12 months** ● **Specifies retention of penetration testing results and remediation activities results.**	Google has PCI DSS compliance responsibility for dedicated internal Google Production and management network systems.	For computer resources that are provided by Google to customers as part of a customer's GCP project. the PCI compliance of those resources is the customer's responsibility.
11.3.1	Perform external penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).	Google is responsible for vulnerability scans, penetration tests and testing for unauthorized wireless access points on the systems and infrastructure underlying GCP in compliance with the requirements of section 11.	GCP customers are responsible for performing vulnerability scans and penetration tests on customer deployed instances on GCP in compliance with the requirements of section 11.

11.3.2	Perform internal penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).	Google is responsible for vulnerability scans, penetration tests and testing for unauthorized wireless access points on the systems and infrastructure underlying GCP in compliance with the requirements of section 11.	GCP customers are responsible for performing vulnerability scans and penetration tests on customer deployed instances on GCP in compliance with the requirements of section 11.
11.3.3	Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.	Google is responsible for vulnerability scans, penetration tests and testing for unauthorized wireless access points on the systems and infrastructure underlying GCP in compliance with the requirements of section 11.	GCP customers are responsible for performing vulnerability scans and penetration tests on customer deployed instances on GCP in compliance with the requirements of section 11.
11.3.4	If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of- scope systems from in-scope systems.	Google is responsible for vulnerability scans, penetration tests and testing for unauthorized wireless access points on the systems and infrastructure underlying GCP in compliance with the requirements of section 11.	GCP customers are responsible for performing vulnerability scans and penetration tests on customer deployed instances on GCP in compliance with the requirements of section 11.
11.4	**Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.**	Google is responsible for intrusion detection of Google Cloud systems and infrastructure underlying GCP in compliance with the requirements of section 11.	GCP customers are responsible for **i**ntrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into their environment.

11.5	**Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. Note: For change- detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file- integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).**	Google is responsible for change-detection mechanisms on the systems and infrastructure underlying GCP in compliance with the requirements of section 11.	GCP customers are responsible for change-detection mechanisms for their environment.
11.5.1	Implement a process to respond to any alerts generated by the change-detection solution.	Google is responsible for change-detection mechanisms on the systems and infrastructure underlying GCP in compliance with the requirements of section 11.	GCP customers are responsible for change-detection mechanisms for their environment.
11.6	**Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties.**	Google is responsible for security policies and operational procedures for GCP in compliance with the requirements of section 11.	GCP customers are responsible for security policies and operational procedures for their environment in compliance with the requirements of section 11.

Product Specific Customer Considerations

Product	Requirement	PCI-DSS Requirement	Additional Customer Responsibility
Cloud Security Scanner	11.2.2	Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved.	Customers should only use Test environment credentials to run scans.

Requirement 12: Maintain Policy that Addresses Information Security for all Personnel

Requirement	Description	GCP	Customer
12.1	**Establish, publish, maintain, and disseminate a security policy.**	Google is responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and infrastructure underlying GCP in compliance with the requirements in section 12.	GCP customers are responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and instances deployed by customers on GCP.
12.1.1	Review the security policy at least annually and update the policy when the environment changes.	Google is responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and infrastructure underlying GCP in compliance with the requirements in section 12.	GCP customers are responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and instances deployed by customers on GCP.
12.2	**Implement a risk-assessment process that:** ● **Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.)** ● **Identifies critical assets, threats, and vulnerabilities, and** ● **Results in a formal risk assessment.**	Google is responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and infrastructure underlying GCP in compliance with the requirements in section 12.	GCP customers are responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and instances deployed by customers on GCP.
12.3	**Develop usage policies for critical technologies and define**	Google is responsible for establishing,	GCP customers are responsible for

	proper use of these technologies. Ensure these usage policies require the following:	maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and infrastructure underlying GCP in compliance with the requirements in section 12.	establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and instances deployed by customers on GCP.
12.3.1	Explicit approval by authorized parties.	Google is responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and infrastructure underlying GCP in compliance with the requirements in section 12.	GCP customers are responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and instances deployed by customers on GCP.
12.3.2	Authentication for use of the technology.	Google is responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and infrastructure underlying GCP in compliance with the requirements in section 12.	GCP customers are responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and instances deployed by customers on GCP.
12.3.3	Authentication for use of the technology.	Google is responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and infrastructure underlying GCP in compliance with the requirements in section 12.	GCP customers are responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and instances deployed by customers on GCP.

12.3.4	A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices).	Google is responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and infrastructure underlying GCP in compliance with the requirements in section 12.	GCP customers are responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and instances deployed by customers on GCP.
12.3.5	Acceptable uses of the technology.	Google is responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and infrastructure underlying GCP in compliance with the requirements in section 12.	GCP customers are responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and instances deployed by customers on GCP.
12.3.6	Acceptable network locations for the technologies.	Google is responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and infrastructure underlying GCP in compliance with the requirements in section 12.	GCP customers are responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and instances deployed by customers on GCP.
12.3.7	List of company-approved products.	Google is responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and infrastructure underlying GCP in	GCP customers are responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and instances deployed by

		compliance with the requirements in section 12.	customers on GCP.
12.3.8	Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity.	Google is responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and infrastructure underlying GCP in compliance with the requirements in section 12.	GCP customers are responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and instances deployed by customers on GCP.
12.3.9	Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use.	Google is responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and infrastructure underlying GCP in compliance with the requirements in section 12.	GCP customers are responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and instances deployed by customers on GCP.
12.3.10	For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements.	Google is responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and infrastructure underlying GCP in compliance with the requirements in section 12.	GCP customers are responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and instances deployed by customers on GCP.
12.4	**Ensure that the security policy and procedures clearly define**	Google is responsible for establishing,	GCP customers are responsible for

	information security responsibilities for all personnel.	maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and infrastructure underlying GCP in compliance with the requirements in section 12.	establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and instances deployed by customers on GCP.
12.5	**Assign to an individual or team the following information security management responsibilities:**	Google has PCI DSS compliance responsibility for dedicated internal Google Production and management network systems.	For computer resources that are provided by Google to customers as part of a customer's GCP project. the PCI compliance of those resources is the customer's responsibility.
12.5.1	Establish, document, and distribute security policies and procedures.	Google maintains a highly trained and professional security team and has implementation a security awareness program for all applicable personnel in compliance with section 12 requirements to manage security for all systems and infrastructure underlying GCP.	GCP customers are responsible for maintaining an information security team and implementing security awareness programs in compliance with section 12 for all customer deployed instances on GCP
12.5.2	Monitor and analyze security alerts and information, and distribute to appropriate personnel.	Google maintains a highly trained and professional security team and has implementation a security awareness program for all applicable personnel in compliance with section 12 requirements to manage security for all systems and infrastructure underlying GCP.	GCP customers are responsible for maintaining an information security team and implementing security awareness programs in compliance with section 12 for all customer deployed instances on GCP

12.5.3	Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.	Google maintains a highly trained and professional security team and has implementation a security awareness program for all applicable personnel in compliance with section 12 requirements to manage security for all systems and infrastructure underlying GCP.	GCP customers are responsible for maintaining an information security team and implementing security awareness programs in compliance with section 12 for all customer deployed instances on GCP
12.5.4	Administer user accounts, including additions, deletions, and modifications.	Google maintains a highly trained and professional security team and has implementation a security awareness program for all applicable personnel in compliance with section 12 requirements to manage security for all systems and infrastructure underlying GCP.	GCP customers are responsible for maintaining an information security team and implementing security awareness programs in compliance with section 12 for all customer deployed instances on GCP
12.5.5	Monitor and control all access to data.	Google is responsible for monitoring access to data by Google staff.	Customers of GCP are responsible for monitoring and controlling their users and or staff. Users including vendors and consumers as applicable got he GCP customer.
12.6	**Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security.**	Google maintains a highly trained and professional security team and has implementation a security awareness program for all applicable personnel in compliance with section 12 requirements to manage security for all systems and infrastructure underlying GCP.	GCP customers are responsible for maintaining an information security team and implementing security awareness programs in compliance with section 12 for all customer deployed instances on GCP

12.6.1	Educate personnel upon hire and at least annually.	Google maintains a highly trained and professional security team and has implementation a security awareness program for all applicable personnel in compliance with section 12 requirements to manage security for all systems and infrastructure underlying GCP.	GCP customers are responsible for maintaining an information security team and implementing security awareness programs in compliance with section 12 for all customer deployed instances on GCP
12.6.2	Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.	Google maintains a highly trained and professional security team and has implementation a security awareness program for all applicable personnel in compliance with section 12 requirements to manage security for all systems and infrastructure underlying GCP.	GCP customers are responsible for maintaining an information security team and implementing security awareness programs in compliance with section 12 for all customer deployed instances on GCP
12.7	**Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.)**	Google has implemented appropriate screening for its personnel which complies with section 12 requirements.	GCP customers are responsible for implementing screening on their applicable personnel in relation to their PCI DSS scope.
12.8	**Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:**		
12.8.1	Maintain a list of service providers.	Google does not share customer data with third party providers. Google is responsible	GCP customers are responsible for complying with this requirement as

		for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and infrastructure underlying GCP in compliance with the requirements in section 12.	applicable to them when cardholder data is shared with third parties.
12.8.2	Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.	Google does not share customer data with third party providers. Google is responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and infrastructure underlying GCP in compliance with the requirements in section 12.	GCP customers are responsible for complying with this requirement as applicable to them when cardholder data is shared with third parties.
12.8.3	Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.	Google does not share customer data with third party providers. Google is responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and infrastructure underlying GCP in compliance with the requirements in section 12.	GCP customers are responsible for complying with this requirement as applicable to them when cardholder data is shared with third parties.
12.8.4	Maintain a program to monitor service providers' PCI DSS compliance status at least annually.	Google does not share customer data with third party providers. Google is responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and infrastructure	GCP customers are responsible for complying with this requirement as applicable to them when cardholder data is shared with third parties.

		underlying GCP in compliance with the requirements in section 12.	
12.8.5	Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.	Google does not share customer data with third party providers. Google is responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and infrastructure underlying GCP in compliance with the requirements in section 12.	GCP customers are responsible for complying with this requirement as applicable to them when cardholder data is shared with third parties.
12.9	**Additional requirement for service providers only: Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.**	See Google's Data Processing and Security terms for GCP.	N/A
12.10	**Implement an incident response plan. Be prepared to respond immediately to a system breach.**	Google has implemented a detailed incident response plan for all systems and infrastructure underlying GCP in compliance with section 12 requirements.	Customers are responsible for implementing an incident response plan in compliance with section 12 requirements for all customer deployed instances and data on GCP.
12.10.1	Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum:	Google has implemented a detailed incident response plan for all systems and infrastructure underlying GCP in	Customers are responsible for implementing an incident response plan in compliance with section 12 requirements

	• Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum • Specific incident response procedures • Business recovery and continuity procedures • Data backup processes • Analysis of legal requirements for reporting compromises • Coverage and responses of all critical system components • Reference or inclusion of incident response procedures from the payment brands	compliance with section 12 requirements.	for all customer deployed instances and data on GCP.
12.10.2	Test the plan at least annually.	Google has implemented a detailed incident response plan for all systems and infrastructure underlying GCP in compliance with section 12 requirements.	Customers are responsible for implementing an incident response plan in compliance with section 12 requirements for all customer deployed instances and data on GCP.
12.10.3	Designate specific personnel to be available on a 24/7 basis to respond to alerts.	Google has implemented a detailed incident response plan for all systems and infrastructure underlying GCP in compliance with section 12 requirements.	Customers are responsible for implementing an incident response plan in compliance with section 12 requirements for all customer deployed instances and data on GCP.
12.10.4	Provide appropriate training to staff with security breach response responsibilities.	Google has implemented a detailed incident response plan for all systems and infrastructure underlying GCP in compliance with section 12 requirements.	Customers are responsible for implementing an incident response plan in compliance with section 12 requirements for all customer deployed instances and data on GCP.

12.10.5	Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems.	Google has implemented a detailed incident response plan for all systems and infrastructure underlying GCP in compliance with section 12 requirements.	Customers are responsible for implementing an incident response plan in compliance with section 12 requirements for all customer deployed instances and data on GCP.
12.10.6	Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.	Google has implemented a detailed incident response plan for all systems and infrastructure underlying GCP in compliance with section 12 requirements.	Customers are responsible for implementing an incident response plan in compliance with section 12 requirements for all customer deployed instances and data on GCP.

Appendix

Additional Requirements for Entities using SSL/early TLS

Requirement	PCI-DSS Requirement	Additional Customer Responsibility
A2.1	Where POS POI terminals (and the SSL/TLS termination points to which they connect) use SSL and/or early TLS, the entity must either: Confirm the devices are not susceptible to any known exploits for those protocols. ***Or:*** Have a formal Risk Mitigation and Migration Plan in place.	N/A no POS/POI devices in scope.
A2.2	Entities with existing implementations (other than as allowed in A.2.1) that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place.	GCP customers are responsible for complying with this requirement for any virtual machines, applications, services or databases deployed by them on GCP.
A2.3	***Additional Requirement for Service Providers Only:*** All service providers must provide a secure service offering by June 30, 2016.	Google has implemented controls for secure administrative access for the Google production infrastructure underlying GCP GCP Customers are responsible for configuring their apps hosted on Google Cloud Platform such that it doesn't accept TLS1.0 requests from their app users. Example: Connections between Customer Instances and End-User

			GCP Customers wishing to disable 3DES or TLS 1.0 for web-based access to the covered services will need to file a support case referencing issue #73300651 and requesting 3DES or TLS 1.0 be disabled for their managed accounts. Google will then apply a policy to user accounts managed under the applicable GCP domain preventing sign in when the user is on a connection using 3DES or TLS 1.0. Example: Connections between Customer administrators and Google's Cloud Console GCP customers are responsible for configuring their clients to disallow connections via TLS 1.0 Example: Connections between Customer and their third-parties.

Product Specific Customer Considerations

Product	Requirement	PCI-DSS Requirement	Additional Customer Responsibility
Google App Engine	A2.3	***Additional Requirement for Service Providers Only:*** All service providers must provide a secure service offering by June 30, 2016.	GCP App Engine Customers can file a support ticket to disable TLS 1.0 for their custom domain. It is a customer responsibility to re-route HTTPS requests from their *.appspot.com address to their custom domain.