Google Cloud Platform: PCI DSS v4.0 Shared Responsibility Matrix

May 2023

Introduction

Google provides its customers with a secure-by-design foundation through the deployment of a variety of innovative technologies and processes on Google Cloud Platform (GCP). GCP has been independently assessed against Payment Card Industry Data Security Standard (PCI DSS) 4.0 requirements for its products and underlying infrastructure. Google offers customers a great deal of control over their GCP projects; Google does not control the security of the operating system, packages or applications that are deployed by customers on GCP. It is the customer's responsibility to comply with the requirements of PCI DSS that relate to customer-deployed operating systems, packages and applications. Additionally, the customer is responsible for configurations in multi-cloud or hybrid cloud environments that exist outside the GCP boundary.

Google complies with the PCI DSS requirements set forth for a level 1 Service Provider. This document outlines the requirements that Google complies with on behalf of its customers, who in turn may leverage GCP to deliver PCI-compliant environments. If a requirement is not included in this document, then GCP is not performing that requirement for its customers. Customers should note that while certain requirements are the sole responsibility of Google, some are the sole responsibility of the customer, and others are a shared responsibility between both parties. Customers using GCP products as part of their cardholder data environment must deploy services in a PCI-compliant manner. Google recommends 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; the Multi-tenant Service Provider.
Google Cloud Platform (GCP) responsibility	**The requirement in question is the responsibility of, and implemented by, Google.** A Qualified Security Assessor (QSA) has assessed and validated these requirements and found GCP to be compliant with PCI-DSS v4.0. These requirements, which support a customer's PCI DSS compliance status 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 are the responsibility of GCP customers to implement and not applicable to Google. Customers bear sole responsibility to meet their own PCI DSS compliance for these requirements.
Shared responsibility	**Both the customer and Google are responsible for implementing elements of the requirement.** A QSA has assessed and validated that GCP is compliant with PCI DSS v4.0 for these specific requirements. However, GCP customers share some responsibility and must act to meet their own PCI DSS compliance for these requirements.
Service Provider	The Service Provider, as defined by the applicable requirement, is Google.
Multi-tenant Service Provider	The Multi-tenant Service Provider, as defined by the applicable requirement, is Google.

Google Cloud Products

The responsibility matrix in this document provides customers with compliance guidance across four product categories that are core to PCI DSS compliance: ‘Compute’, ‘Networking’, ‘Storage’, and ‘Security & Identity’. Additional detail on the products that Google offers in these categories is accessible here: https://cloud.google.com/products/. For information on the full list of certified GCP products, please refer to https://cloud.google.com/security/compliance/pci-dss.

Responsibility Matrix

PCI DSS 4.0 Requirements	PCI DSS 3.2.1	GCP	Customer	Compute	Networking	Storage	Security & Identity	Google Responsibility Summary
Requirement 1: Install and Maintain Network Security Controls								
1.1.1 All security policies and operational procedures that are identified in Requirement 1 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	1.5		x	Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Not Applicable	Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Not Applicable
1.1.2 Roles and responsibilities for performing activities in Requirement 1 are documented, assigned, and understood.	1.1.5	x	x	Customers are responsible for documenting and assigning roles and responsibilities for applicable activities. Roles and responsibilities must be understood by assigned individuals.	Customers are responsible for documenting and assigning roles and responsibilities for applicable activities. Roles and responsibilities must be understood by assigned individuals.	Not Applicable	Customers are responsible for documenting and assigning roles and responsibilities for applicable activities. Roles and responsibilities must be understood by assigned individuals.	Google has documented and assigned roles and responsibilities for applicable activities. Roles and responsibilities are understood by assigned individuals.
1.2.1 Configuration standards for NSC rulesets are: • Defined. • Implemented. • Maintained.	1.1	x	x	Customers are responsible for formalizing change control processes around approval and testing of network connections, i.e. GCP firewall rules that impact their VPC networks and VM instances.	Customers are responsible for formalizing change control processes around approval and testing of network connections, i.e. GCP firewall rules that impact their VPC networks and VM instances.	Not Applicable	Customers are responsible for formalizing change control processes around approval and testing of network connections, i.e. GCP firewall rules that impact their VPC networks and VM instances.	Google's internal production network and systems have been assessed against and comply with this requirement.
1.2.2 All changes to network connections and to configurations of NSCs are approved and managed in accordance with the change control process defined at Requirement 6.5.1.	1.1.1	x	x	Customers are responsible for formalizing change control processes around approval and testing of network connections, i.e. GCP firewall rules that impact their VPC networks and VM instances.	Customers are responsible for formalizing change control processes around approval and testing of network connections, i.e. GCP firewall rules that impact their VPC networks and VM instances.	Not Applicable	Customers are responsible for formalizing change control processes around approval and testing of network connections, i.e. GCP firewall rules that impact their VPC networks and VM instances.	Google's internal production network and systems have been assessed against and comply with this requirement.
1.2.3 An accurate network diagram(s) is maintained that shows all connections between the CDE and other networks, including any wireless networks.	1.1.2		x	Customers are responsible for maintaining their own network diagrams specific to their CDE that identify all connections between their CDE and any other networks. Customers may use Network Intelligence Center to assist in meeting this requirement.	Customers are responsible for maintaining their own network diagrams specific to their CDE that identify all connections between their CDE and any other networks. Customers may use Network Intelligence Center to assist in meeting this requirement.	Not Applicable	Customers are responsible for maintaining their own network diagrams specific to their CDE that identify all connections between their CDE and any other networks. Customers may use Network Intelligence Center to assist in meeting this requirement.	Not Applicable
1.2.4 An accurate data-flow diagram(s) is maintained that meets the following: • Shows all account data flows across systems and networks. • Updated as needed upon changes to the environment.	1.1.3		x	Customers are responsible for maintaining their own data-flow diagrams specific to their CDE. Customers may use Network Intelligence Center to assist in meeting this requirement.	Customers are responsible for maintaining their own data-flow diagrams specific to their CDE. Customers may use Network Intelligence Center to assist in meeting this requirement.	Not Applicable	Customers are responsible for maintaining their own data-flow diagrams specific to their CDE Customers may use Network Intelligence Center to assist in meeting this requirement..	Not Applicable

PCI DSS 4.0 Requirements	PCI DSS 3.2.1	GCP	Customer	Compute	Networking	Storage	Security & Identity	Google Responsibility Summary
1.2.5 All services, protocols, and ports allowed are identified, approved, and have a defined business need.	1.1.6	x	x	Customers are responsible for documenting and justifying the GCP firewall rules for each inbound/outbound rule. Customers are responsible for documenting ports and protocols in use, with justification for inbound/outbound rules in place. Customers are responsible for identifying insecure services and implementing appropriate controls and security features to limit the risk of the protocols from being used.	Customers are responsible for documenting and justifying the GCP firewall rules for each inbound/outbound rule. Customers are responsible for documenting ports and protocols in use, with justification for inbound/outbound rules in place. Customers are responsible for identifying insecure services and implementing appropriate controls and security features to limit the risk of the protocols from being used.	Not Applicable	Customers are responsible for documenting and justifying the GCP firewall rules for each inbound/outbound rule. Customers are responsible for documenting ports and protocols in use, with justification for inbound/outbound rules in place. Customers are responsible for identifying insecure services and implementing appropriate controls and security features to limit the risk of the protocols from being used.	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.
1.2.6 Security features are defined and implemented for all services, protocols, and ports that are in use and considered to be insecure, such that the risk is mitigated.	1.1.6	x	x	Customers are responsible for documenting and justifying the GCP firewall rules for each inbound/outbound rule. Customers are responsible for documenting ports and protocols in use, with justification for inbound/outbound rules in place. Customers are responsible for identifying insecure services and implementing appropriate controls and security features to limit the risk of the protocols from being used.	Customers are responsible for documenting and justifying the GCP firewall rules for each inbound/outbound rule. Customers are responsible for documenting ports and protocols in use, with justification for inbound/outbound rules in place. Customers are responsible for identifying insecure services and implementing appropriate controls and security features to limit the risk of the protocols from being used.	Not Applicable	Customers are responsible for documenting and justifying the GCP firewall rules for each inbound/outbound rule. Customers are responsible for documenting ports and protocols in use, with justification for inbound/outbound rules in place. Customers are responsible for identifying insecure services and implementing appropriate controls and security features to limit the risk of the protocols from being used.	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.
1.2.7 Configurations of NSCs are reviewed at least once every six months to confirm they are relevant and effective.	1.1.7	x	x	Customers are responsible for performing bi-annual firewall reviews of their virtual firewalls and other network technology and services that are used to filter traffic into the CDE. This includes but may not be limited to VM instances, storage buckets, and VPC firewall rules.	Customers are responsible for performing bi-annual firewall reviews of their virtual firewalls and other network technology and services that are used to filter traffic into the CDE. This includes but may not be limited to VM instances, storage buckets, and VPC firewall rules.	Not Applicable	Customers are responsible for performing bi-annual firewall reviews of their virtual firewalls and other network technology and services that are used to filter traffic into the CDE. This includes but may not be limited to VM instances, storage buckets, and VPC firewall rules.	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.
1.2.8 Configuration files for NSCs are: • Secured from unauthorized access. • Kept consistent with active network configurations.	1.2.2	x		Not Applicable	Not Applicable	Not Applicable	Not Applicable	Google's internal production network and systems have been assessed against and comply with this requirement. Customers using GCP can rely on the GCP AOC for router configuration security and synchronization.
1.3.1 Inbound traffic to the CDE is restricted as follows: • To only traffic that is necessary. • All other traffic is specifically denied.	1.2.1, 1.3.4	x	x	Customers are responsible for implementing GCP firewall rules and limiting inbound/outbound traffic to only business justified and necessary traffic. Customers must define explicit GCP firewall rules and deny all other traffic. Customers are responsible for verifying inbound and outbound traffic for their CDE which includes VPC networks, GCS, and VM instances. Customers are responsible for	Customers are responsible for implementing GCP firewall rules and limiting inbound/outbound traffic to only business justified and necessary traffic. Customers must define explicit GCP firewall rules and deny all other traffic. Customers are responsible for verifying inbound and outbound traffic for their CDE which includes VPC networks, GCS, and VM instances. Customers are responsible for	Not Applicable	Customers are responsible for implementing GCP firewall rules and limiting inbound/outbound traffic to only business justified and necessary traffic. Customers must define explicit GCP firewall rules and deny all other traffic. Customers are responsible for verifying inbound and outbound traffic for their CDE which includes VPC networks, GCS, and VM instances. Customers are responsible for	Google restricts inbound and outbound traffic to only that which is necessary. All other traffic is specifically denied

PCI DSS 4.0 Requirements	PCI DSS 3.2.1	GCP	Customer	Compute	Networking	Storage	Security & Identity	Google Responsibility Summary
				denying any traffic that is not explicitly required for the GCP Product to function.	denying any traffic that is not explicitly required for the GCP Product to function.		denying any traffic that is not explicitly required for the GCP Product to function.	
1.3.2 Outbound traffic from the CDE is restricted as follows: • To only traffic that is necessary. • All other traffic is specifically denied.	1.2.1, 1.3.4	x	x	Customers are responsible for implementing GCP firewall rules and limiting inbound/outbound traffic to only business justified and necessary traffic. Customers must define explicit GCP firewall rules and deny all other traffic. Customers are responsible for verifying inbound and outbound traffic for their CDE which includes VPC networks, GCS, and VM instances. Customers are responsible for denying any traffic that is not explicitly required for the GCP Product to function.	Customers are responsible for implementing GCP firewall rules and limiting inbound/outbound traffic to only business justified and necessary traffic. Customers must define explicit GCP firewall rules and deny all other traffic. Customers are responsible for verifying inbound and outbound traffic for their CDE which includes VPC networks, GCS, and VM instances. Customers are responsible for denying any traffic that is not explicitly required for the GCP Product to function.	Not Applicable	Customers are responsible for implementing GCP firewall rules and limiting inbound/outbound traffic to only business justified and necessary traffic. Customers must define explicit GCP firewall rules and deny all other traffic. Customers are responsible for verifying inbound and outbound traffic for their CDE which includes VPC networks, GCS, and VM instances. Customers are responsible for denying any traffic that is not explicitly required for the GCP Product to function.	Google restricts inbound and outbound traffic to only that which is necessary. All other traffic is specifically denied
1.3.3 NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that: • All wireless traffic from wireless networks into the CDE is denied by default. • Only wireless traffic with an authorized business purpose is allowed into the CDE.	1.2.3	x	x	Customers that use wireless networks are responsible for isolating their cardholder data environment from those wireless networks.	Customers that use wireless networks are responsible for isolating their cardholder data environment from those wireless networks.	Not Applicable	Customers that use wireless networks are responsible for isolating their cardholder data environment from those wireless networks.	GCP maintains the perimeter firewalls and controls traffic between wireless networks and systems in GCP data centers.
1.4.1 NSCs are implemented between trusted and untrusted networks.	1.3	x	x	Customers are responsible for implementing firewall rules and limiting ingress traffic to defined ports and protocols necessary for VM instances within their DMZ or equivalent.	Customers are responsible for implementing firewall rules and limiting ingress traffic to defined ports and protocols and denying all other traffic. Customers must implement defined networks and not the default network with pre-configured rules and utilize secure ports and protocols as well as restricting inbound/outbound connectivity to that which is necessary and deny-all other traffic.	Not Applicable	Customers are responsible for implementing perimeter firewalls and configuring firewall rules and ACLs for their in-scope GCP Products. Customers are responsible for developing appropriate firewall rules or using additional firewall technologies to develop appropriate DMZ and internal networks.	Google restricts inbound and outbound traffic to only that which is necessary. All other traffic is specifically denied
1.4.2 Inbound traffic from untrusted networks to trusted networks is restricted to: • Communications with system components that are authorized to provide publicly accessible services, protocols, and ports. • Stateful responses to communications initiated by system components in a trusted network. • All other traffic is denied.	1.3.1, 1.3.2, 1.3.5	x	x	Customers are responsible for implementing firewall rules and limiting ingress traffic to defined ports and protocols necessary for VM instances within their DMZ or equivalent.	Customers are responsible for implementing firewall rules and limiting ingress traffic to defined ports and protocols and denying all other traffic. Customers must implement defined networks and not the default network with pre-configured rules and utilize secure ports and protocols as well as restricting inbound/outbound connectivity to that which is necessary and deny-all other traffic.	Not Applicable	Customers are responsible for determining system components that are authorized to provide publicly accessible services, protocols, and ports; restricting any inbound traffic accordingly.	Google restricts inbound and outbound traffic to only that which is necessary. All other traffic is specifically denied. GCP firewalls perform stateful packet inspection by default and customers can rely on the GCP AOC for compliance with stateful packet inspection controls.
1.4.3 Anti-spoofing measures are implemented to detect and block forged source IP addresses from entering the trusted network.	1.3.3	x		Not Applicable	Not Applicable	Not Applicable	Not Applicable	GCP firewalls perform anti-spoofing by default. As such, customers can

PCI DSS 4.0 Requirements	PCI DSS 3.2.1	GCP	Customer	Compute	Networking	Storage	Security & Identity	Google Responsibility Summary
								rely on the GCP AOC for compliance with anti-spoofing controls.
1.4.4 System components that store cardholder data are not directly accessible from untrusted networks.	1.3.6		x	Customers are responsible for developing appropriate firewall rules or using additional firewall technologies to develop appropriate internal networks and ensure that any systems storing CHD are located within private internal networks.	Customers are responsible for developing appropriate firewall rules or using additional firewall technologies to develop appropriate internal networks and ensure that any systems storing CHD are located within private internal networks.	Customers are responsible for implementing GCS public access prevention to ensure that buckets storing CHD are inaccessible from public networks.	Customers are responsible for developing appropriate firewall rules or using additional firewall technologies to develop appropriate internal networks and ensure that any systems storing CHD are located within private internal networks.	Not Applicable
1.4.5 The disclosure of internal IP addresses and routing information is limited to only authorized parties.	1.3.7	x	x	Customers are responsible for developing appropriate configuration on GCP VM instances to prevent the disclosure of IP Addresses and routing information.	Customers are responsible for developing appropriate configuration on GCP VM instances to prevent the disclosure of IP Addresses and routing information.	Not Applicable	Customers are responsible for developing appropriate configuration on GCP VM instances to prevent the disclosure of IP Addresses and routing information.	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.
1.5.1 Security controls are implemented on any computing devices, including company- and employee-owned devices, that connect to both untrusted networks (including the Internet) and the CDE as follows: • Specific configuration settings are defined to prevent threats being introduced into the entity's network. • Security controls are actively running. • Security controls are not alterable by users of the computing devices unless specifically documented and authorized by management on a case-by-case basis for a limited period.	1.4		x	Customers are responsible for implementing personal firewall rules for systems with direct connectivity to the Internet for systems used to manage VM instances within GCP.	Customers are responsible for implementing personal firewall rules for systems with direct connectivity to the Internet for systems used to manage VM instances within GCP.	Not Applicable	Customers are responsible for implementing personal firewall rules for systems with direct connectivity to the Internet for systems used to manage VM instances within GCP.	Not Applicable
Requirement 2: Apply Secure Configurations to All System Components								
2.1.1 All security policies and operational procedures that are identified in Requirement 2 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	2.5		x	Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Not Applicable
2.1.2 Roles and responsibilities for performing activities in Requirement 2 are documented, assigned, and understood.	*New*	x	x	Customers are responsible for documenting and assigning roles and responsibilities for applicable activities. Roles and responsibilities must be understood by assigned individuals.	Customers are responsible for documenting and assigning roles and responsibilities for applicable activities. Roles and responsibilities must be understood by assigned individuals.	Customers are responsible for documenting and assigning roles and responsibilities for applicable activities. Roles and responsibilities must be understood by assigned individuals.	Customers are responsible for documenting and assigning roles and responsibilities for applicable activities. Roles and responsibilities must be understood by assigned individuals.	Google has documented and assigned roles and responsibilities for applicable activities. Roles and responsibilities are understood by assigned individuals.

PCI DSS 4.0 Requirements	PCI DSS 3.2.1	GCP	Customer	Compute	Networking	Storage	Security & Identity	Google Responsibility Summary
2.2.1 Configuration standards are developed, implemented, and maintained to: • Cover all system components. • Address all known security vulnerabilities. • Be consistent with industry-accepted system hardening standards or vendor hardening recommendations. • Be updated as new vulnerability issues are identified, as defined in Requirement 6.3.1. • Be applied when new systems are configured and verified as in place before or immediately after a system component is connected to a production environment.	2.2	x	x	Customers are responsible for documenting, developing and implementing configuration standards for the GCP products in use that are within the CDE. This includes configuration standards for VM instances, VPC networks, and storage buckets based on industry standards and hardening guidelines. Hardened images can assist with this requirement and may be available from the Google Cloud Marketplace.	Customers are responsible for documenting, developing and implementing configuration standards for the GCP products in use that are within the CDE. This includes configuration standards for VM instances, VPC networks, and storage buckets based on industry standards and hardening guidelines. Hardened images can assist with this requirement and may be available from the Google Cloud Marketplace.	Customers are responsible for documenting, developing and implementing configuration standards for the GCP products in use that are within the CDE. This includes configuration standards for VM instances, VPC networks, and storage buckets based on industry standards and hardening guidelines. Hardened images can assist with this requirement and may be available from the Google Cloud Marketplace.	Customers are responsible for documenting, developing and implementing configuration standards for the GCP products in use that are within the CDE. This includes configuration standards for VM instances, VPC networks, and storage buckets based on industry standards and hardening guidelines. Hardened images can assist with this requirement and may be available from the Google Cloud Marketplace.	Google has implemented configuration standards for the infrastructure underlying GCP products in scope that comply with this PCI DSS requirement.
2.2.2 Vendor default accounts are managed as follows: • If the vendor default account(s) will be used, the default password is changed per Requirement 8.3.6. • If the vendor default account(s) will not be used, the account is removed or disabled.	2.1	x	x	Customers are responsible for changing vendor-supplied defaults on GCP products as applicable deployed within the customers CDE.	Customers are responsible for changing vendor-supplied defaults on GCP products as applicable deployed within the customers CDE.	Customers are responsible for changing vendor-supplied defaults on GCP products as applicable deployed within the customers CDE.	Customers are responsible for changing vendor-supplied defaults on GCP products as applicable deployed within the customers CDE.	Google has PCI DSS compliance responsibility for dedicated internal Google Production and management network systems.
2.2.3 Primary functions requiring different security levels are managed as follows: • Only one primary function exists on a system component, OR • Primary functions with differing security levels that exist on the same system component are isolated from each other, OR • Primary functions with differing security levels on the same system component are all secured to the level required by the function with the highest security need.	2.2.1	x	x	Customers are responsible for ensuring that only one primary function is implemented per customer-managed GCP product.	Customers are responsible for ensuring that only one primary function is implemented per customer-managed GCP product.	Customers are responsible for ensuring that only one primary function is implemented per customer-managed GCS bucket.	Customers are responsible for ensuring that only one primary function is implemented per customer-managed GCP product.	Google has implemented configuration standards for the infrastructure underlying GCP products in scope that comply with this PCI DSS requirement.
2.2.4 Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality is removed or disabled.	2.2.2, 2.2.5	x	x	Customers are responsible for documenting the functional and security configuration standards of GCP services used within the CDE to ensure that the secure state designed for the service can be maintained.	Customers are responsible for documenting the functional and security configuration standards of GCP services used within the CDE to ensure that the secure state designed for the service can be maintained.	Customers are responsible for documenting the functional and security configuration standards of GCP services used within the CDE to ensure that the secure state designed for the service can be maintained.	Customers are responsible for documenting the functional and security configuration standards of GCP services used within the CDE to ensure that the secure state designed for the service can be maintained.	Google has implemented configuration standards for the infrastructure underlying GCP products in scope that comply with this PCI DSS requirement.
2.2.5 If any insecure services, protocols, or daemons are present: • Business justification is documented. • Additional security features are documented and implemented that reduce the risk of using insecure services, protocols, or daemons.	2.2.3		x	Customers are responsible for documenting, developing and implementing configuration standards, including additional features required for any insecure service, protocol, daemon, etc. employed on the GCP products deployed within the CDE.	Customers are responsible for documenting, developing and implementing configuration standards, including additional features required for any insecure service, protocol, daemon, etc. employed on the GCP products deployed within the CDE.	Customers are responsible for documenting, developing and implementing configuration standards, including additional features required for any insecure service, protocol, daemon, etc. employed on the GCP products deployed within the CDE.	Customers are responsible for documenting, developing and implementing configuration standards, including additional features required for any insecure service, protocol, daemon, etc. employed on the GCP products deployed within the CDE.	Not Applicable. GCP does not implement insecure services, protocols or daemons.
2.2.6 System security parameters are configured to prevent misuse.	2.2.4	x	x	Customers are responsible for documenting the functional and security configuration standards of GCP services used within the CDE to ensure that the secure state designed for the service can be maintained.	Customers are responsible for documenting the functional and security configuration standards of GCP services used within the CDE to ensure that the secure state designed for the service can be maintained.	Customers are responsible for documenting the functional and security configuration standards of GCP services used within the CDE to ensure that the secure state designed for the service can be maintained.	Customers are responsible for documenting the functional and security configuration standards of GCP services used within the CDE to ensure that the secure state designed for the service can be maintained.	Google has implemented configuration standards for the infrastructure underlying GCP products in scope that comply with this PCI DSS requirement.

PCI DSS 4.0 Requirements	PCI DSS 3.2.1	GCP	Customer	Compute	Networking	Storage	Security & Identity	Google Responsibility Summary
2.2.7 All non-console administrative access is encrypted using strong cryptography.	2.3	x	x	Customers are responsible for ensuring secure connection with GCP via a strong TLS connection, per PCI DSS requirements. Customers are also responsible for ensuring secure communication for administrative access to the server instances including Windows Remote Desktop (RDP) using "High Encryption" or "FIPS compatible" encryption settings or SSH v2 or above and appropriate SSH keys.	Customers are responsible for ensuring secure connection with GCP via a strong TLS connection, per PCI DSS requirements. Customers are also responsible for ensuring secure communication for administrative access to the server instances including Windows Remote Desktop (RDP) using "High Encryption" or "FIPS compatible" encryption settings or SSH v2 or above and appropriate SSH keys.	Customers are responsible for ensuring secure connection with GCP via a strong TLS connection, per PCI DSS requirements. Customers are also responsible for ensuring secure communication for administrative access to the server instances including Windows Remote Desktop (RDP) using "High Encryption" or "FIPS compatible" encryption settings or SSH v2 or above and appropriate SSH keys.	Customers are responsible for ensuring secure connection with GCP via a strong TLS connection, per PCI DSS requirements. Customers are also responsible for ensuring secure communication for administrative access to the server instances including Windows Remote Desktop (RDP) using "High Encryption" or "FIPS compatible" encryption settings or SSH v2 or above and appropriate SSH keys.	Google has implemented controls for secure administrative access for the in-scope production infrastructure underlying GCP.
2.3.1 For wireless environments connected to the CDE or transmitting account data, all wireless vendor defaults are changed at installation or are confirmed to be secure, including but not limited to: • Default wireless encryption keys. • Passwords on wireless access points. • SNMP defaults. • Any other security-related wireless vendor defaults.	2.1.1		x	GCP does not host any wireless networks that transmit cardholder data. Customers are responsible for management of their networks, including those with wireless connectivity.	GCP does not host any wireless networks that transmit cardholder data. Customers are responsible for management of their networks, including those with wireless connectivity.	GCP does not host any wireless networks that transmit cardholder data. Customers are responsible for management of their networks, including those with wireless connectivity.	GCP does not host any wireless networks that transmit cardholder data. Customers are responsible for management of their networks, including those with wireless connectivity.	Not Applicable. No wireless networks are connected to the in-scope GCP environment.
2.3.2 For wireless environments connected to the CDE or transmitting account data, wireless encryption keys are changed as follows: • Whenever personnel with knowledge of the key leave the company or the role for which the knowledge was necessary. • Whenever a key is suspected of or known to be compromised.	2.1.1		x	GCP does not host any wireless networks that transmit cardholder data. Customers are responsible for management of their networks, including those with wireless connectivity.	GCP does not host any wireless networks that transmit cardholder data. Customers are responsible for management of their networks, including those with wireless connectivity.	GCP does not host any wireless networks that transmit cardholder data. Customers are responsible for management of their networks, including those with wireless connectivity.	GCP does not host any wireless networks that transmit cardholder data. Customers are responsible for management of their networks, including those with wireless connectivity.	Not Applicable. No wireless networks are connected to the in-scope GCP environment.
Requirement 3: Protect Stored Account Data								
3.1.1 All security policies and operational procedures that are identified in Requirement 3 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	3.7		x	Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Not Applicable
3.1.2 Roles and responsibilities for performing activities in Requirement 3 are documented, assigned, and understood.	*New*	x	x	Customers are responsible for documenting and assigning roles and responsibilities for applicable activities. Roles and responsibilities must be understood by assigned individuals.	Customers are responsible for documenting and assigning roles and responsibilities for applicable activities. Roles and responsibilities must be understood by assigned individuals.	Customers are responsible for documenting and assigning roles and responsibilities for applicable activities. Roles and responsibilities must be understood by assigned individuals.	Customers are responsible for documenting and assigning roles and responsibilities for applicable activities. Roles and responsibilities must be understood by assigned individuals.	Google has documented and assigned roles and responsibilities for applicable activities. Roles and responsibilities are understood by assigned individuals.

PCI DSS 4.0 Requirements	PCI DSS 3.2.1	GCP	Customer	Compute	Networking	Storage	Security & Identity	Google Responsibility Summary
3.2.1 Account data storage is kept to a minimum through implementation of data retention and disposal policies, procedures, and processes that include at least the following: • Coverage for all locations of stored account data. • Coverage for any sensitive authentication data (SAD) stored prior to completion of authorization. This bullet is a best practice until its effective date; refer to Applicability Notes below for details. • Limiting data storage amount and retention time to that which is required for legal or regulatory, and/or business requirements. • Specific retention requirements for stored account data that defines length of retention period and includes a documented business justification. • Processes for secure deletion or rendering account data unrecoverable when no longer needed per the retention policy. • A process for verifying, at least once every three months, that stored account data exceeding the defined retention period has been securely deleted or rendered unrecoverable.	3.1		x	Customers are responsible for maintaining appropriate data retention policies, procedures, and processes for maintaining PCI Data Security Standard (PCI DSS) requirements.	Customers are responsible for maintaining appropriate data retention policies, procedures, and processes for maintaining PCI Data Security Standard (PCI DSS) requirements.	Customers are responsible for maintaining appropriate data retention policies, procedures, and processes for maintaining PCI Data Security Standard (PCI DSS) requirements. Customers may use bucket lock policies to retain data and create immutable policies for data contained in the storage bucket.	Customers are responsible for maintaining appropriate data retention policies, procedures, and processes for maintaining PCI Data Security Standard (PCI DSS) requirements.	Not Applicable
3.3.1 SAD is not retained after authorization, even if encrypted. All sensitive authentication data received is rendered unrecoverable upon completion of the authorization process.	3.2		x	Customers are responsible for maintaining appropriate data retention policies, procedures, and processes for maintaining PCI Data Security Standard (PCI DSS) requirements.	Customers are responsible for maintaining appropriate data retention policies, procedures, and processes for maintaining PCI Data Security Standard (PCI DSS) requirements.	Customers are responsible for maintaining appropriate data retention policies, procedures, and processes for maintaining PCI Data Security Standard (PCI DSS) requirements. Customers may use bucket lock policies to retain data and create immutable policies for data contained in the storage bucket.	Customers are responsible for maintaining appropriate data retention policies, procedures, and processes for maintaining PCI Data Security Standard (PCI DSS) requirements.	Not Applicable
3.3.1.1 The full contents of any track are not retained upon completion of the authorization process.	3.2.1		x	Customers are responsible for maintaining appropriate data retention policies, procedures, and processes for maintaining PCI Data Security Standard (PCI DSS) requirements.	Not Applicable	Customers are responsible for maintaining appropriate data retention policies, procedures, and processes for maintaining PCI Data Security Standard (PCI DSS) requirements. Customers may use bucket lock policies to retain data and create immutable policies for data contained in the storage bucket.	Customers are responsible for maintaining appropriate data retention policies, procedures, and processes for maintaining PCI Data Security Standard (PCI DSS) requirements.	Not Applicable
3.3.1.2 The card verification code is not retained upon completion of the authorization process.	3.2.2		x	Customers are responsible for maintaining appropriate data retention policies, procedures, and processes for maintaining PCI Data Security Standard (PCI DSS) requirements.	Not Applicable	Customers are responsible for maintaining appropriate data retention policies, procedures, and processes for maintaining PCI Data Security Standard (PCI DSS) requirements. Customers may use bucket lock policies to retain data and create immutable policies for data contained in the storage bucket.	Customers are responsible for maintaining appropriate data retention policies, procedures, and processes for maintaining PCI Data Security Standard (PCI DSS) requirements.	Not Applicable

PCI DSS 4.0 Requirements	PCI DSS 3.2.1	GCP	Customer	Compute	Networking	Storage	Security & Identity	Google Responsibility Summary
3.3.1.3 The personal identification number (PIN) and the PIN block are not retained upon completion of the authorization process.	3.2.3		x	Customers are responsible for maintaining appropriate data retention policies, procedures, and processes for maintaining PCI Data Security Standard (PCI DSS) requirements.	Not Applicable	Customers are responsible for maintaining appropriate data retention policies, procedures, and processes for maintaining PCI Data Security Standard (PCI DSS) requirements. Customers may use bucket lock policies to retain data and create immutable policies for data contained in the storage bucket.	Customers are responsible for maintaining appropriate data retention policies, procedures, and processes for maintaining PCI Data Security Standard (PCI DSS) requirements.	Not Applicable
3.3.2 SAD that is stored electronically prior to completion of authorization is encrypted using strong cryptography.	*New*		x	Customers are responsible for maintaining appropriate encryption technologies and key management processes in alignment with PCI Data Security Standard (PCI DSS) requirements.	Not Applicable	Customers are responsible for maintaining appropriate encryption technologies and key management processes in alignment with PCI Data Security Standard (PCI DSS) requirements.	Customers are responsible for maintaining appropriate encryption technologies and key management processes in alignment with PCI Data Security Standard (PCI DSS) requirements. Customers are responsible for the creation, usage, and management of customer encryption keys in accordance with PCI DSS controls for these GCP Products.	Not Applicable
3.3.3 Additional requirement for issuers and companies that support issuing services and store sensitive authentication data: Any storage of sensitive authentication data is: • Limited to that which is needed for a legitimate issuing business need and is secured. • Encrypted using strong cryptography. This bullet is a best practice until its effective date; refer to Applicability Notes below for details.	3.2.a, 3.2.b		x	Customers are responsible for maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI DSS requirements.	Not Applicable	Customers are responsible for maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI DSS requirements.	Customers are responsible for maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI DSS requirements. Customers are responsible for the creation, usage, and management of customer encryption keys in accordance with PCI DSS controls for these GCP Products.	Not Applicable
3.4.1 PAN is masked when displayed (the BIN and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the BIN and last four digits of the PAN.	3.3		x	Customers are responsible for maintaining appropriate data retention policies, procedures, and processes for maintaining PCI Data Security Standard (PCI DSS) requirements.	Customers are responsible for maintaining appropriate data retention policies, procedures, and processes for maintaining PCI Data Security Standard (PCI DSS) requirements.	Customers are responsible for maintaining appropriate data retention policies, procedures, and processes for maintaining PCI Data Security Standard (PCI DSS) requirements.	Customers are responsible for maintaining appropriate data retention policies, procedures, and processes for maintaining PCI Data Security Standard (PCI DSS) requirements. Customers may use Cloud DLP to mask the PAN and enforce access controls to prevent personnel without legitimate business need from viewing the PAN.	Not Applicable
3.4.2 When using remote-access technologies, technical controls prevent copy and/or relocation of PAN for all personnel, except for those with documented, explicit authorization and a legitimate, defined business need.	12.3.10		x	Customers are responsible for their use of remote access technologies, including the implementation of any technical controls preventing the copying or relocation of PAN.	Customers are responsible for their use of remote access technologies, including the implementation of any technical controls preventing the copying or relocation of PAN.	Customers are responsible for their use of remote access technologies, including the implementation of any technical controls preventing the copying or relocation of PAN.	Customers are responsible for their use of remote access technologies, including the implementation of any technical controls preventing the copying or relocation of PAN. Customers may use Cloud DLP to mask the PAN and enforce access controls to prevent personnel without	Not Applicable

PCI DSS 4.0 Requirements	PCI DSS 3.2.1	GCP	Customer	Compute	Networking	Storage	Security & Identity	Google Responsibility Summary
							legitimate business need from viewing the PAN.	
3.5.1 PAN is rendered unreadable anywhere it is stored by using any of the following approaches: • One-way hashes based on strong cryptography of the entire PAN. • Truncation (hashing cannot be used to replace the truncated segment of PAN). – If hashed and truncated versions of the same PAN, or different truncation formats of the same PAN, are present in an environment, additional controls are in place such that the different versions cannot be correlated to reconstruct the original PAN. • Index tokens. • Strong cryptography with associated key- management processes and procedures.	3.4		x	Customers are responsible for their use of remote access technologies, including the implementation of any technical controls preventing the copying or relocation of PAN.	Not Applicable	Customers are responsible for rendering PAN unreadable and any associated key-management processes and procedures.	Customers are responsible for rendering PAN unreadable and any associated key-management processes and procedures. Customers may use Cloud DLP to mask the PAN and enforce access controls to prevent personnel without legitimate business need from viewing the PAN.	Not Applicable
3.5.1.1 Hashes used to render PAN unreadable (per the first bullet of Requirement 3.5.1) are keyed cryptographic hashes of the entire PAN, with associated key-management processes and procedures in accordance with Requirements 3.6 and 3.7.	*New*		x	Customers are responsible for rendering PAN unreadable and any associated key-management processes and procedures.	Not Applicable	Customers are responsible for rendering PAN unreadable and any associated key-management processes and procedures.	Customers are responsible for rendering PAN unreadable and any associated key-management processes and procedures. Customers may use Cloud DLP to mask the PAN and enforce access controls to prevent personnel without legitimate business need from viewing the PAN.	Not Applicable
3.5.1.2 If disk-level or partition-level encryption (rather than file-, column-, or field-level database encryption) is used to render PAN unreadable, it is implemented only as follows: • On removable electronic media OR • If used for non-removable electronic media, PAN is also rendered unreadable via another mechanism that meets Requirement 3.5.1.	*New*		x	Customers are responsible for rendering PAN unreadable and any associated key-management processes and procedures.	Not Applicable	Customers are responsible for rendering PAN unreadable and any associated key-management processes and procedures.	Customers are responsible for rendering PAN unreadable and any associated key-management processes and procedures. Customers may use Cloud DLP to mask the PAN and enforce access controls to prevent personnel without legitimate business need from viewing the PAN.	Not Applicable
3.5.1.3 If disk-level or partition-level encryption is used (rather than file-, column-, or field–level database encryption) to render PAN unreadable, it is managed as follows: • Logical access is managed separately and independently of native operating system authentication and access control mechanisms. • Decryption keys are not associated with user accounts. • Authentication factors (passwords, passphrases, or cryptographic keys) that allow access to unencrypted data are stored securely.	3.4.1		x	Customers are responsible for their use of remote access technologies, including the implementation of any technical controls preventing the copying or relocation of PAN.	Not Applicable	Customers are responsible for their use of remote access technologies, including the implementation of any technical controls preventing the copying or relocation of PAN.	Customers are responsible for their use of remote access technologies, including the implementation of any technical controls preventing the copying or relocation of PAN. Such technical controls include Cloud DLP for identification and masking of PAN and authentication factors; Secret Manager for secure storage of authentication factors; and Cloud KMS for management of cryptographic keys.	Not Applicable

PCI DSS 4.0 Requirements	PCI DSS 3.2.1	GCP	Customer	Compute	Networking	Storage	Security & Identity	Google Responsibility Summary
3.6.1 Procedures are defined and implemented to protect cryptographic keys used to protect stored account data against disclosure and misuse that include: • Access to keys is restricted to the fewest number of custodians necessary. • Key-encrypting keys are at least as strong as the data-encrypting keys they protect. • Key-encrypting keys are stored separately from data-encrypting keys. • Keys are stored securely in the fewest possible locations and forms.	3.5		x	Customers are responsible for maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI DSS requirements.	Not Applicable	Customers are responsible for maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI DSS requirements.	Customers are responsible for maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI DSS requirements. Customers are responsible for the creation, usage, and management of customer encryption keys in accordance with PCI DSS controls for these GCP Products.	Not Applicable
3.6.1.1 Additional requirement for service providers only: A documented description of the cryptographic architecture is maintained that includes: • Details of all algorithms, protocols, and keys used for the protection of stored account data, including key strength and expiry date. • Preventing the use of the same cryptographic keys in production and test environments. This bullet is a best practice until its effective date; refer to Applicability Notes below for details. • Description of the key usage for each key. • Inventory of any hardware security modules (HSMs), key management systems (KMS), and other secure cryptographic devices (SCDs) used for key management, including type and location of devices, as outlined in Requirement 12.3.4.	3.5.1	x	x	Customers are responsible for maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI DSS requirements.	Not Applicable	Customers are responsible for maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI DSS requirements.	Customers are responsible for maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI DSS requirements. Customers are responsible for the creation, usage, and management of customer encryption keys in accordance with PCI DSS controls for these GCP Products.	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.
3.6.1.2 Secret and private keys used to encrypt/decrypt stored account data are stored 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 (SCD), such as a hardware security module (HSM) or PTS-approved point-of-interaction device. • As at least two full-length key components or key shares, in accordance with an industry-accepted method.	3.5.3		x	Customers are responsible for maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI DSS requirements.	Not Applicable	Customers are responsible for maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI DSS requirements.	Customers are responsible for maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI DSS requirements. Customers are responsible for the creation, usage, and management of customer encryption keys in accordance with PCI DSS controls for these GCP Products.	Not Applicable
3.6.1.3 Access to cleartext cryptographic key components is restricted to the fewest number of custodians necessary.	3.5.2	x	x	Customers are responsible for maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI DSS requirements.	Not Applicable	Customers are responsible for maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI DSS requirements.	Customers are responsible for maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI DSS requirements. Customers are responsible for the creation, usage, and management of customer encryption keys in accordance with PCI DSS controls for these GCP Products.	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.

PCI DSS 4.0 Requirements	PCI DSS 3.2.1	GCP	Customer	Compute	Networking	Storage	Security & Identity	Google Responsibility Summary
3.6.1.4 Cryptographic keys are stored in the fewest possible locations.	3.5.4	x	x	Customers are responsible for maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI DSS requirements.	Not Applicable	Customers are responsible for maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI DSS requirements.	Customers are responsible for maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI DSS requirements. Customers are responsible for the creation, usage, and management of customer encryption keys in accordance with PCI DSS controls for these GCP Products.	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.
3.7.1 Key-management policies and procedures are implemented to include generation of strong cryptographic keys used to protect stored account data.	3.6		x	Customers are responsible for maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI DSS requirements.	Not Applicable	Customers are responsible for maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI DSS requirements.	Customers are responsible for maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI DSS requirements. Customers are responsible for the creation, usage, and management of customer encryption keys in accordance with PCI DSS controls for these GCP Products.	Not Applicable
3.7.2 Key-management policies and procedures are implemented to include secure distribution of cryptographic keys used to protect stored account data.	3.6.2		x	Customers are responsible for maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI DSS requirements.	Not Applicable	Customers are responsible for maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI DSS requirements.	Customers are responsible for maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI DSS requirements. Customers are responsible for the creation, usage, and management of customer encryption keys in accordance with PCI DSS controls for these GCP Products.	Not Applicable
3.7.3 Key-management policies and procedures are implemented to include secure storage of cryptographic keys used to protect stored account data.	3.6.3		x	Customers are responsible for maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI DSS requirements.	Not Applicable	Customers are responsible for maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI DSS requirements.	Customers are responsible for maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI DSS requirements. Customers are responsible for the creation, usage, and management of customer encryption keys in accordance with PCI DSS controls for these GCP Products.	Not Applicable

PCI DSS 4.0 Requirements	PCI DSS 3.2.1	GCP	Customer	Compute	Networking	Storage	Security & Identity	Google Responsibility Summary
3.7.4 Key management policies and procedures are implemented for cryptographic key changes for keys that have reached the end of their cryptoperiod, as defined by the associated application vendor or key owner, and based on industry best practices and guidelines, including the following: • A defined cryptoperiod for each key type in use. • A process for key changes at the end of the defined cryptoperiod.	3.6.4	x	x	Customers are responsible for maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI DSS requirements.	Not Applicable	Customers are responsible for maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI DSS requirements.	Customers are responsible for maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI DSS requirements. Customers are responsible for the creation, usage, and management of customer encryption keys in accordance with PCI DSS controls for these GCP Products.	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.
3.7.5 Key management policies procedures are implemented to include the retirement, replacement, or destruction of keys used to protect stored account data, as deemed necessary when: • The key has reached the end of its defined cryptoperiod. • The integrity of the key has been weakened, including when personnel with knowledge of a cleartext key component leaves the company, or the role for which the key component was known. • The key is suspected of or known to be compromised. Retired or replaced keys are not used for encryption operations.	3.6.5		x	Customers are responsible for maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI DSS requirements.	Not Applicable	Customers are responsible for maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI DSS requirements.	Customers are responsible for maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI DSS requirements. Customers are responsible for the creation, usage, and management of customer encryption keys in accordance with PCI DSS controls for these GCP Products.	Not Applicable
3.7.6 Where manual cleartext cryptographic key-management operations are performed by personnel, key-management policies and procedures are implemented include managing these operations using split knowledge and dual control.	3.6.6		x	Customers are responsible for maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI DSS requirements.	Not Applicable	Customers are responsible for maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI DSS requirements.	Customers are responsible for maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI DSS requirements. Customers are responsible for the creation, usage, and management of customer encryption keys in accordance with PCI DSS controls for these GCP Products.	Not Applicable. Google does not use clear text cryptographic key management. This is a customer responsibility.
3.7.7 Key management policies and procedures are implemented to include the prevention of unauthorized substitution of cryptographic keys.	3.6.7	x	x	Customers are responsible for maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI DSS requirements.	Not Applicable	Customers are responsible for maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI DSS requirements.	Customers are responsible for maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI DSS requirements. Customers are responsible for the creation, usage, and management of customer encryption keys in accordance with PCI DSS controls for these GCP Products.	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.

PCI DSS 4.0 Requirements	PCI DSS 3.2.1	GCP	Customer	Compute	Networking	Storage	Security & Identity	Google Responsibility Summary
3.7.8 Key management policies and procedures are implemented to include that cryptographic key custodians formally acknowledge (in writing or electronically) that they understand and accept their key-custodian responsibilities.	3.6.8		x	Customers are responsible for maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI DSS requirements.	Not Applicable	Customers are responsible for maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI DSS requirements.	Customers are responsible for maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI DSS requirements. Customers are responsible for the creation, usage, and management of customer encryption keys in accordance with PCI DSS controls for these GCP Products.	Not Applicable
3.7.9 Additional requirement for service providers only: Where a service provider shares cryptographic keys with its customers for transmission or storage of account data, guidance on secure transmission, storage and updating of such keys is documented and distributed to the service provider's customers.	3.5.1	x	x	Customers are responsible for maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI DSS requirements.	Not Applicable	Customers are responsible for maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI DSS requirements.	Customers are responsible for maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI DSS requirements. Customers are responsible for the creation, usage, and management of customer encryption keys in accordance with PCI DSS controls for these GCP Products.	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.
Requirement 4: Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks								
4.1.1 All security policies and operational procedures that are identified in Requirement 4 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	4.3		x	Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Not Applicable.
4.1.2 Roles and responsibilities for performing activities in Requirement 4 are documented, assigned, and understood.	*New*		x	Customers are responsible for documenting and assigning roles and responsibilities for applicable activities. Roles and responsibilities must be understood by assigned individuals.	Customers are responsible for documenting and assigning roles and responsibilities for applicable activities. Roles and responsibilities must be understood by assigned individuals.	Customers are responsible for documenting and assigning roles and responsibilities for applicable activities. Roles and responsibilities must be understood by assigned individuals.	Customers are responsible for documenting and assigning roles and responsibilities for applicable activities. Roles and responsibilities must be understood by assigned individuals.	Not Applicable.
4.2.1 Strong cryptography and security protocols are implemented as follows to safeguard PAN during transmission over open, public networks: • Only trusted keys and certificates are accepted. • Certificates used to safeguard PAN during transmission over open, public networks are confirmed as valid and are not expired or revoked. This bullet is a best practice until its effective date; refer to applicability notes below for details. • The protocol in use supports only secure versions or configurations and does not support fallback to, or use of insecure versions, algorithms, key sizes, or implementations.	4.1		x	Customers are responsible for strong cryptography and security protocols for connections to any storage system that is transmitting cardholder data. Customers are responsible for ensuring the data is encrypted in transit over open, public networks.	Customers are responsible for strong cryptography and security protocols for connections to any storage system that is transmitting cardholder data. Customers are responsible for ensuring the data is encrypted in transit over open, public networks.	Customers are responsible for strong cryptography and security protocols for connections to any storage system that is transmitting cardholder data. Customers are responsible for ensuring the data is encrypted in transit over open, public networks.	Customers are responsible for strong cryptography and security protocols for connections to any storage system that is transmitting cardholder data. Customers are responsible for ensuring the data is encrypted in transit over open, public networks.	Not Applicable.

PCI DSS 4.0 Requirements	PCI DSS 3.2.1	GCP	Customer	Compute	Networking	Storage	Security & Identity	Google Responsibility Summary
• The encryption strength is appropriate for the encryption methodology in use.								
4.2.1.1 An inventory of the entity's trusted keys and certificates used to protect PAN during transmission is maintained.	*New*		x	Customers are responsible for maintaining an inventory of keys and certificates used to protect PAN during transmission.	Customers are responsible for maintaining an inventory of keys and certificates used to protect PAN during transmission.	Customers are responsible for maintaining an inventory of keys and certificates used to protect PAN during transmission.	Customers are responsible for maintaining an inventory of keys and certificates used to protect PAN during transmission. Such an inventory may be established and maintained with Secret Manager.	Not Applicable.
4.2.1.2 Wireless networks transmitting PAN or connected to the CDE use industry best practices to implement strong cryptography for authentication and transmission.	4.1.1		x	Customers are responsible for management of their networks, including those with wireless connectivity.	Customers are responsible for management of their networks, including those with wireless connectivity.	Customers are responsible for management of their networks, including those with wireless connectivity.	Customers are responsible for management of their networks, including those with wireless connectivity.	Not Applicable.
4.2.2 PAN is secured with strong cryptography whenever it is sent via end-user messaging technologies.	4.2		x	Customers are responsible for the use of any end-user messaging technologies for transmitting PAN.	Customers are responsible for the use of any end-user messaging technologies for transmitting PAN.	Customers are responsible for the use of any end-user messaging technologies for transmitting PAN.	Customers are responsible for the use of any end-user messaging technologies for transmitting PAN.	Not Applicable.
Requirement 5: Protect All Systems and Networks from Malicious Software								
5.1.1 All security policies and operational procedures that are identified in Requirement 5 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	5.4		x	Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Not Applicable
5.1.2 Roles and responsibilities for performing activities in Requirement 5 are documented, assigned, and understood.	*New*	x	x	Customers are responsible for documenting and assigning roles and responsibilities for applicable activities. Roles and responsibilities must be understood by assigned individuals.	Customers are responsible for documenting and assigning roles and responsibilities for applicable activities. Roles and responsibilities must be understood by assigned individuals.	Customers are responsible for documenting and assigning roles and responsibilities for applicable activities. Roles and responsibilities must be understood by assigned individuals.	Customers are responsible for documenting and assigning roles and responsibilities for applicable activities. Roles and responsibilities must be understood by assigned individuals.	Google has documented and assigned roles and responsibilities for applicable activities. Roles and responsibilities are understood by assigned individuals.
5.2.1 An anti-malware solution(s) is deployed on all system components, except for those system components identified in periodic evaluations per Requirement 5.2.3 that concludes the system components are not at risk from malware.	5.1	x	x	Customers are responsible for managing anti-virus software or programs for any customer-managed VM instances. Customers are responsible for centrally managing malicious code protection mechanisms for their compute infrastructure. This includes interconnections with systems outside of the Google Cloud PCI DSS scope.	Not Applicable	Not Applicable	Customers are responsible for managing anti-virus software or programs for any customer-managed VM instances. Security Command Center Premium customers may identify malware including cryptocurrency mining, kernel tampering, and execution of binaries or libraries. Customers may use Shielded VMs to protect themselves from rootkits and bootkits.	Google is responsible for the implementation of malware protection in the underlying GCP infrastructure in compliance with this requirement. Google is not responsible for the implementation of malware protection within any customer deployed instances on GCP.
5.2.2 The deployed anti-malware solution(s): • Detects all known types of malware. • Removes, blocks, or contains all known types of malware.	5.1.1	x	x	Customers are responsible for managing anti-virus software or programs for any customer-managed VM instances. Customers are responsible for centrally managing malicious code protection mechanisms for their compute infrastructure. This includes	Not Applicable	Not Applicable	Customers are responsible for managing anti-virus software or programs for any customer-managed VM instances. Security Command Center Premium customers may identify malware including cryptocurrency mining, kernel tampering, and execution of binaries	Google is responsible for the implementation of malware protection in the underlying GCP infrastructure in compliance with this requirement. Google is not responsible for the implementation of malware protection within any customer deployed instances on GCP.

PCI DSS 4.0 Requirements	PCI DSS 3.2.1	GCP	Customer	Compute	Networking	Storage	Security & Identity	Google Responsibility Summary
				interconnections with systems outside of the Google Cloud PCI DSS scope.			or libraries. Customers may use Shielded VMs to protect themselves from rootkits and bootkits.	
5.2.3 Any system components that are not at risk for malware are evaluated periodically to include the following: • A documented list of all system components not at risk for malware. • Identification and evaluation of evolving malware threats for those system components. • Confirmation whether such system components continue to not require anti-malware protection.	5.1.2	x	x	Customers are responsible for managing anti-virus software or programs for any customer-managed VM instances. Customers are responsible for centrally managing malicious code protection mechanisms for their compute infrastructure. This includes interconnections with systems outside of the Google Cloud PCI DSS scope.	Not Applicable	Not Applicable	Customers are responsible for managing anti-virus software or programs for any customer-managed VM instances.	Google is responsible for the implementation of malware protection in the underlying GCP infrastructure in compliance with this requirement. Google is not responsible for the implementation of malware protection within any customer deployed instances on GCP.
5.2.3.1 The frequency of periodic evaluations of system components identified as not at risk for malware is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.	*New*		x	Customers are responsible for conducting a targeted risk analysis of their control environment and determining control frequency to meet applicable PCI DSS requirements.	Customers are responsible for conducting a targeted risk analysis of their control environment and determining control frequency to meet applicable PCI DSS requirements.	Customers are responsible for conducting a targeted risk analysis of their control environment and determining control frequency to meet applicable PCI DSS requirements.	Customers are responsible for conducting a targeted risk analysis of their control environment and determining control frequency to meet applicable PCI DSS requirements.	Not Applicable
5.3.1 The anti-malware solution(s) is kept current via automatic updates.	5.2	x	x	Customers are responsible for managing anti-virus software or programs for any customer-managed VM instances. Customers are responsible for centrally managing malicious code protection mechanisms for their compute infrastructure. This includes interconnections with systems outside of the Google Cloud PCI DSS scope.	Not Applicable	Not Applicable	Customers are responsible for managing anti-virus software or programs for any customer-managed VM instances.	Google is responsible for the implementation of malware protection in the underlying GCP infrastructure in compliance with this requirement. Google is not responsible for the implementation of malware protection within any customer deployed instances on GCP.
5.3.2 The anti-malware solution(s): • Performs periodic scans and active or real-time scans. OR • Performs continuous behavioral analysis of systems or processes.	5.2	x	x	Customers are responsible for managing anti-virus software or programs for any customer-managed VM instances. Customers are responsible for centrally managing malicious code protection mechanisms for their compute infrastructure. This includes interconnections with systems outside of the Google Cloud PCI DSS scope.	Not Applicable	Not Applicable	Customers are responsible for managing anti-virus software or programs for any customer-managed VM instances.	Google is responsible for the implementation of malware protection in the underlying GCP infrastructure in compliance with this requirement. Google is not responsible for the implementation of malware protection within any customer deployed instances on GCP.
5.3.2.1 If periodic malware scans are performed to meet Requirement 5.3.2, the frequency of scans is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.	*New*		x	Customers are responsible for conducting a targeted risk analysis of their control environment and determining control frequency to meet applicable PCI DSS requirements.	Customers are responsible for conducting a targeted risk analysis of their control environment and determining control frequency to meet applicable PCI DSS requirements.	Customers are responsible for conducting a targeted risk analysis of their control environment and determining control frequency to meet applicable PCI DSS requirements.	Customers are responsible for conducting a targeted risk analysis of their control environment and determining control frequency to meet applicable PCI DSS requirements.	Not Applicable

PCI DSS 4.0 Requirements	PCI DSS 3.2.1	GCP	Customer	Compute	Networking	Storage	Security & Identity	Google Responsibility Summary
5.3.3 For removable electronic media, the anti- malware solution(s): • Performs automatic scans of when the media is inserted, connected, or logically mounted, OR • Performs continuous behavioral analysis of systems or processes when the media is inserted, connected, or logically mounted.	*New*	x	x	Customers are responsible for managing anti-virus software or programs for any customer-managed VM instances. Customers are responsible for centrally managing malicious code protection mechanisms for their compute infrastructure. This includes interconnections with systems outside of the Google Cloud PCI DSS scope.	Not Applicable	Not Applicable	Customers are responsible for managing anti-virus software or programs for any customer-managed VM instances.	Google is responsible for the implementation of malware protection in the underlying GCP infrastructure in compliance with this requirement. Google is not responsible for the implementation of malware protection within any customer deployed instances on GCP.
5.3.4 Audit logs for the anti-malware solution(s) are enabled and retained in accordance with Requirement 10.5.1.	5.2	x	x	Customers are responsible for managing anti-virus software or programs for any customer-managed VM instances. Customers are responsible for centrally managing malicious code protection mechanisms for their compute infrastructure. This includes interconnections with systems outside of the Google Cloud PCI DSS scope.	Not Applicable	Not Applicable	Customers are responsible for managing anti-virus software or programs for any customer-managed VM instances.	Google is responsible for the implementation of malware protection in the underlying GCP infrastructure in compliance with this requirement. Google is not responsible for the implementation of malware protection within any customer deployed instances on GCP.
5.3.5 Anti-malware mechanisms cannot be disabled or altered by users, unless specifically documented, and authorized by management on a case-by-case basis for a limited time period.	5.3	x	x	Customers are responsible for managing anti-virus software or programs for any customer-managed VM instances. Customers are responsible for centrally managing malicious code protection mechanisms for their compute infrastructure. This includes interconnections with systems outside of the Google Cloud PCI DSS scope.	Not Applicable	Not Applicable	Customers are responsible for managing anti-virus software or programs for any customer-managed VM instances.	Google is responsible for the implementation of malware protection in the underlying GCP infrastructure in compliance with this requirement. Google is not responsible for the implementation of malware protection within any customer deployed instances on GCP.
5.4.1 Processes and automated mechanisms are in place to detect and protect personnel against phishing attacks.	*New*		x	Customers are responsible for managing an anti-phishing program using automated mechanisms to detect attacks.	Customers are responsible for managing an anti-phishing program using automated mechanisms to detect attacks.	Customers are responsible for managing an anti-phishing program using automated mechanisms to detect attacks.	Customers are responsible for managing an anti-phishing program using automated mechanisms to detect attacks.	Not Applicable
Requirement 6: Develop and Maintain Secure Systems and Software								
6.1.1 All security policies and operational procedures that are identified in Requirement 6 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	6.7		x	Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Not Applicable
6.1.2 Roles and responsibilities for performing activities in Requirement 6 are documented, assigned, and understood.	*New*	x	x	Customers are responsible for documenting and assigning roles and responsibilities for applicable	Customers are responsible for documenting and assigning roles and responsibilities for applicable	Customers are responsible for documenting and assigning roles and responsibilities for applicable	Customers are responsible for documenting and assigning roles and responsibilities for applicable	Google has documented and assigned roles and responsibilities for applicable activities. Roles and

PCI DSS 4.0 Requirements	PCI DSS 3.2.1	GCP	Customer	Compute	Networking	Storage	Security & Identity	Google Responsibility Summary
				activities. Roles and responsibilities must be understood by assigned individuals.	activities. Roles and responsibilities must be understood by assigned individuals.	activities. Roles and responsibilities must be understood by assigned individuals.	activities. Roles and responsibilities must be understood by assigned individuals.	responsibilities are understood by assigned individuals.
6.2.1 Bespoke and custom software are developed securely, as follows: • Based on industry standards and/or best practices for secure development. • In accordance with PCI DSS (for example, secure authentication and logging). • Incorporating consideration of information security issues during each stage of the software development lifecycle.	6.3	x	x	Customers are responsible to maintain software development standards aligned with PCI requirements for applications developed and deployed on customer-managed VM instances.	Not Applicable	Not Applicable	Customers are responsible to maintain software development standards aligned with PCI requirements for applications developed and deployed on customer-managed VM instances.	Google is responsible for protecting the systems and infrastructure underlying GCP from vulnerabilities in compliance with this requirement.
6.2.2 Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows: • On software security relevant to their job function and development languages. • Including secure software design and secure coding techniques. • Including, if security testing tools are used, how to use the tools for detecting vulnerabilities in software.	6.5		x	Customers are responsible to maintain software development standards aligned with PCI requirements for applications developed and deployed on customer-managed VM instances.	Not Applicable	Not Applicable	Customers are responsible to maintain software development standards aligned with PCI requirements for applications developed and deployed on customer-managed VM instances.	Not Applicable
6.2.3 Bespoke and custom software is reviewed prior to being released into production or to customers, to identify and correct potential coding vulnerabilities, as follows: • Code reviews ensure code is developed according to secure coding guidelines. • Code reviews look for both existing and emerging software vulnerabilities. • Appropriate corrections are implemented prior to release.	6.3.2	x	x	Customers are responsible to maintain software development standards aligned with PCI requirements for applications developed and deployed on customer-managed VM instances.	Not Applicable	Not Applicable	Customers are responsible to maintain software development standards aligned with PCI requirements for applications developed and deployed on customer-managed VM instances. Customers may use Security Command Center Premium to identify vulnerabilities and misconfigurations.	Google is responsible for protecting the systems and infrastructure underlying GCP from vulnerabilities in compliance with this requirement.
6.2.3.1 If manual code reviews are performed for bespoke and custom software prior to release to production, code changes are: • Reviewed by individuals other than the originating code author, and who are knowledgeable about code-review techniques and secure coding practices. • Reviewed and approved by management prior to release.	6.3.2	x	x	Customers are responsible to maintain software development standards aligned with PCI requirements for applications developed and deployed on customer-managed VM instances.	Not Applicable	Not Applicable	Customers are responsible to maintain software development standards aligned with PCI requirements for applications developed and deployed on customer-managed VM instances.	Google is responsible for protecting the systems and infrastructure underlying GCP from vulnerabilities in compliance with this requirement.

PCI DSS 4.0 Requirements	PCI DSS 3.2.1	GCP	Customer	Compute	Networking	Storage	Security & Identity	Google Responsibility Summary
6.2.4 Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in bespoke and custom software, including but not limited to the following: • Injection attacks, including SQL, LDAP, XPath, or other command, parameter, object, fault, or injection-type flaws. • Attacks on data and data structures, including attempts to manipulate buffers, pointers, input data, or shared data. • Attacks on cryptography usage, including attempts to exploit weak, insecure, or inappropriate cryptographic implementations, algorithms, cipher suites, or modes of operation. • Attacks on business logic, including attempts to abuse or bypass application features and functionalities through the manipulation of APIs, communication protocols and channels, client- side functionality, or other system/application functions and resources. This includes cross-site scripting (XSS) and cross-site request forgery (CSRF). • Attacks on access control mechanisms, including attempts to bypass or abuse identification, authentication, or authorization mechanisms, or attempts to exploit weaknesses in the implementation of such mechanisms. • Attacks via any “high-risk” vulnerabilities identified in the vulnerability identification process, as defined in Requirement 6.3.1.	6.5.1 – 6.5.10		x	Customers are responsible to maintain software development standards aligned with PCI requirements for applications developed and deployed on customer-managed VM instances.	Not Applicable	Not Applicable	Customers are responsible to maintain software development standards and train developers in secure software development practices aligned with PCI requirements for applications developed and deployed on customer-managed VM instances.	Not Applicable
6.3.1 Security vulnerabilities are identified and managed as follows: • New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). • Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. • Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. • Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.	6.1	x	x	Customers are responsible for establishing a vulnerability management program to identify vulnerabilities using reputable outside sources and assign a risk ranking to those vulnerabilities affecting their VM instances.	Customers are responsible for establishing a vulnerability management program to identify vulnerabilities using reputable outside sources and assign a risk ranking to those vulnerabilities affecting their VPC networks.	Customers are responsible for establishing a vulnerability management program to identify vulnerabilities using reputable outside sources and assign a risk ranking to those vulnerabilities affecting in-scope storage buckets.	Customers are responsible for implementing a formalized vulnerability management process that includes identification of security vulnerabilities using outside sources that are reputable, and assigning a risk ranking to discovered vulnerabilities.	Google is responsible for protecting the systems and infrastructure underlying GCP from vulnerabilities in compliance with this requirement.
6.3.2 An inventory of bespoke and custom software, and third-party software components incorporated into bespoke and custom software is maintained to facilitate vulnerability and patch management.	*New*		x	Customers are responsible for maintaining an inventory of bespoke and custom software, inclusive of third-party software components, to facilitate vulnerability and patch management.	Customers are responsible for maintaining an inventory of bespoke and custom software, inclusive of third-party software components, to facilitate vulnerability and patch management.	Customers are responsible for maintaining an inventory of bespoke and custom software, inclusive of third-party software components, to facilitate vulnerability and patch management.	Customers are responsible for maintaining an inventory of bespoke and custom software, inclusive of third-party software components, to facilitate vulnerability and patch management. Customers may use the Cloud Asset Inventory service to view, monitor, and analyze all Google Cloud	Not Applicable

PCI DSS 4.0 Requirements	PCI DSS 3.2.1	GCP	Customer	Compute	Networking	Storage	Security & Identity	Google Responsibility Summary
							and Anthos assets across projects and services.	
6.3.3 All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows: • Critical or high-security patches/updates (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release. • All other applicable security patches/updates are installed within an appropriate time frame as determined by the entity (for example, within three months of release).	6.2	x	x	Customers are responsible for managing the security patches of their VM instances and installing all applicable security patches within one month of release. Compute Engine OS Patch Management may be used to apply operating system patches across a set of VM instances.	Not Applicable	Not Applicable	Customers are responsible for implementing a formalized patch management process that includes installing all applicable security patches and those flagged as critical within one month of release.	Google is responsible for protecting the systems and infrastructure underlying GCP from vulnerabilities in compliance with this requirement.
6.4.1 For public-facing web applications, new threats and vulnerabilities are addressed on an ongoing basis and these applications are protected against known attacks as follows: • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods as follows: – At least once every 12 months and after significant changes. – By an entity that specializes in application security. – Including, at a minimum, all common software attacks in Requirement 6.2.4. – All vulnerabilities are ranked in accordance with requirement 6.3.1. – All vulnerabilities are corrected. – The application is re-evaluated after the corrections OR • Installing an automated technical solution(s) that continually detects and prevents web-based attacks as follows: – Installed in front of public-facing web applications to detect and prevent web- based attacks. – Actively running and up to date as applicable. – Generating audit logs. – Configured to either block web-based attacks or generate an alert that is immediately investigated.	6.6		x	Customers are responsible for Web Application Filtering or application security reviews for web applications deployed on customer-managed VM instances.	Not Applicable	Not Applicable	Customers are responsible for Web Application Filtering or application security reviews for web applications deployed on customer-managed VM instances. Customers may use Cloud Armor to protect themselves against OWASP Top 10 vulnerabilities and may define web application firewall rules to further protect themselves from web application vulnerabilities.	Not Applicable
6.4.2 For public-facing web applications, an automated technical solution is deployed that continually detects and prevents web-based attacks, with at least the following: • Is installed in front of public-facing web applications and is configured to detect and prevent web-based attacks. • Actively running and up to date as applicable. • Generating audit logs. • Configured to either block web-based attacks or generate an alert that is immediately investigated.	*New*		x	Customers are responsible for deploying automated solutions in front of customer-managed VM instances and configuring them to detect and prevent web-based attacks.	Not Applicable	Not Applicable	Customers are responsible for deploying automated solutions in front of customer-managed VM instances and configuring them to detect and prevent web-based attacks. Customers may use Cloud Armor to protect themselves against OWASP Top 10 vulnerabilities and may define web application firewall rules to further protect themselves from web application vulnerabilities. Cloud Armor can be configured to	Not Applicable

PCI DSS 4.0 Requirements	PCI DSS 3.2.1	GCP	Customer	Compute	Networking	Storage	Security & Identity	Google Responsibility Summary
							generate alerts when attacks are suspected.	
6.4.3 All payment page scripts that are loaded and executed in the consumer's browser are managed as follows: • A method is implemented to confirm that each script is authorized. • A method is implemented to assure the integrity of each script. • An inventory of all scripts is maintained with written justification as to why each is necessary.	*New*		x	Customers are responsible for ensuring that payment page scripts meet PCI DSS requirements.	Not Applicable	Not Applicable	Customers are responsible for ensuring that payment page scripts meet PCI DSS requirements.	Not Applicable
6.5.1 Changes to all system components in the production environment are made according to established procedures that include: • Reason for, and description of, the change. • Documentation of security impact. • Documented change approval by authorized parties. • Testing to verify that the change does not adversely impact system security. • For bespoke and custom software changes, all updates are tested for compliance with Requirement 6.2.4 before being deployed into production. • Procedures to address failures and return to a secure state.	6.4.5		x	Customers are responsible to maintain software development standards, change control processes, and vulnerability management standards aligned with PCI requirements for applications developed and deployed on customer-managed VM instances.	Customers must designate separate VPC networks for development/test and production and enforce appropriate firewall rules ingress and egress with appropriate access controls.	Customers must designate unique storage buckets for development/ test and production; They cannot use the same storage buckets for dev/ test and production environments.	Customers are responsible to maintain software development standards, change control processes, and vulnerability management standards aligned with PCI requirements for applications developed and deployed on customer-managed VM instances. IAM roles and permissions can be used to separate development and test environments.	Not Applicable
6.5.2 Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable.	6.4.6		x	Customers are responsible to maintain software development standards, change control processes, and vulnerability management standards aligned with PCI requirements for applications developed and deployed on customer-managed VM instances.	Customers must designate separate VPC networks for development/test and production and enforce appropriate firewall rules ingress and egress with appropriate access controls.	Customers must designate unique storage buckets for development/ test and production; They cannot use the same storage buckets for dev/ test and production environments.	Customers are responsible to maintain software development standards, change control processes, and vulnerability management standards aligned with PCI requirements for applications developed and deployed on customer-managed VM instances. IAM roles and permissions can be used to separate development and test environments.	Not Applicable
6.5.3 Pre-production environments are separated from production environments and the separation is enforced with access controls.	6.4.1		x	Customers are responsible to maintain software development standards, change control processes, and vulnerability management standards aligned with PCI requirements for applications developed and deployed on customer-managed VM instances.	Customers must designate separate VPC networks for development/test and production and enforce appropriate firewall rules ingress and egress with appropriate access controls.	Customers must designate unique storage buckets for development/ test and production; They cannot use the same storage buckets for dev/ test and production environments.	Customers are responsible to maintain software development standards, change control processes, and vulnerability management standards aligned with PCI requirements for applications developed and deployed on customer-managed VM instances. IAM roles and permissions can be used to separate development and test environments.	Not Applicable

PCI DSS 4.0 Requirements	PCI DSS 3.2.1	GCP	Customer	Compute	Networking	Storage	Security & Identity	Google Responsibility Summary
6.5.4 Roles and functions are separated between production and pre-production environments to provide accountability such that only reviewed and approved changes are deployed.	6.4.2		x	Customers are responsible to maintain software development standards, change control processes, and vulnerability management standards aligned with PCI requirements for applications developed and deployed on customer-managed VM instances.	Customers must designate separate VPC networks for development/test and production and enforce appropriate firewall rules ingress and egress with appropriate access controls.	Customers must designate unique storage buckets for development/ test and production; They cannot use the same storage buckets for dev/ test and production environments.	Customers are responsible to maintain software development standards, change control processes, and vulnerability management standards aligned with PCI requirements for applications developed and deployed on customer-managed VM instances. IAM roles and permissions can be used to separate development and test environments.	Not Applicable
6.5.5 Live PANs are not used in pre-production environments, except where those environments are included in the CDE and protected in accordance with all applicable PCI DSS requirements.	6.4.3		x	Customers are responsible to maintain software development standards, change control processes, and vulnerability management standards aligned with PCI requirements for applications developed and deployed on customer-managed VM instances.	Customers must designate separate VPC networks for development/test and production and enforce appropriate firewall rules ingress and egress with appropriate access controls.	Customers must designate unique storage buckets for development/ test and production; They cannot use the same storage buckets for dev/ test and production environments.	Customers are responsible to maintain software development standards, change control processes, and vulnerability management standards aligned with PCI requirements for applications developed and deployed on customer-managed VM instances. IAM roles and permissions can be used to separate development and test environments.	Not Applicable
6.5.6 Test data and test accounts are removed from system components before the system goes into production.	6.3.1, 6.4.4		x	Customers are responsible to maintain software development standards, change control processes, and vulnerability management standards aligned with PCI requirements for applications developed and deployed on customer-managed VM instances.	Customers must designate separate VPC networks for development/test and production and enforce appropriate firewall rules ingress and egress with appropriate access controls.	Customers must designate unique storage buckets for development/ test and production; They cannot use the same storage buckets for dev/ test and production environments.	Customers are responsible to maintain software development standards, change control processes, and vulnerability management standards aligned with PCI requirements for applications developed and deployed on customer-managed VM instances. IAM roles and permissions can be used to separate development and test environments.	Not Applicable
Requirement 7: Restrict Access to System Components and Cardholder Data by Business Need to Know								
7.1.1 All security policies and operational procedures that are identified in Requirement 7 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	7.3		x	Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Not Applicable
7.1.2 Roles and responsibilities for performing activities in Requirement 7 are documented, assigned, and understood.	*New*	x	x	Customers are responsible for documenting and assigning roles and responsibilities for applicable activities. Roles and responsibilities must be understood by assigned individuals.	Customers are responsible for documenting and assigning roles and responsibilities for applicable activities. Roles and responsibilities must be understood by assigned individuals.	Customers are responsible for documenting and assigning roles and responsibilities for applicable activities. Roles and responsibilities must be understood by assigned individuals.	Customers are responsible for documenting and assigning roles and responsibilities for applicable activities. Roles and responsibilities must be understood by assigned individuals.	Google has documented and assigned roles and responsibilities for applicable activities. Roles and responsibilities are understood by assigned individuals.

PCI DSS 4.0 Requirements	PCI DSS 3.2.1	GCP	Customer	Compute	Networking	Storage	Security & Identity	Google Responsibility Summary
7.2.1 An access control model is defined and includes granting access as follows: • Appropriate access depending on the entity's business and access needs. • Access to system components and data resources that is based on users' job classification and functions. • The least privileges required (for example, user, administrator) to perform a job function.	7.1.1	x	x	Customers are responsible for managing access to all GCP products (GCE, VPC, GCS, etc.) that are included in their CDE. GCP provides various mechanisms for controlling access to the services including IAM for integration with corporate directories and granular access controls to the GCP Management Console.	Customers are responsible for managing access to all GCP products (GCE, VPC, GCS, etc.) that are included in their CDE. GCP provides various mechanisms for controlling access to the services including IAM for integration with corporate directories and granular access controls to the GCP Management Console.	Customers are responsible for managing access to all GCP products (GCE, VPC, GCS, etc.) that are included in their CDE. GCP provides various mechanisms for controlling access to the services including IAM for integration with corporate directories and granular access controls to the GCP Management Console.	Customers are responsible for managing access to all GCP products (GCE, VPC, GCS, etc.) that are included in their CDE. GCP provides various mechanisms for controlling access to the services including IAM for integration with corporate directories and granular access controls to the GCP Management Console.	Google is responsible for implementing access controls in compliance with this requirement for the systems and infrastructure underlying GCP.
7.2.2 Access is assigned to users, including privileged users, based on: • Job classification and function. • Least privileges necessary to perform job responsibilities.	7.1.2, 7.1.3	x	x	Customers are responsible for managing access to all GCP products (GCE, VPC, GCS, etc.) that are included in their CDE. GCP provides various mechanisms for controlling access to the services including IAM for integration with corporate directories and granular access controls to the GCP Management Console.	Customers are responsible for managing access to all GCP products (GCE, VPC, GCS, etc.) that are included in their CDE. GCP provides various mechanisms for controlling access to the services including IAM for integration with corporate directories and granular access controls to the GCP Management Console.	Customers are responsible for managing access to all GCP products (GCE, VPC, GCS, etc.) that are included in their CDE. GCP provides various mechanisms for controlling access to the services including IAM for integration with corporate directories and granular access controls to the GCP Management Console.	Customers are responsible for managing access to all GCP products (GCE, VPC, GCS, etc.) that are included in their CDE. GCP provides various mechanisms for controlling access to the services including IAM for integration with corporate directories and granular access controls to the GCP Management Console.	Google is responsible for implementing access controls in compliance with this requirement for the systems and infrastructure underlying GCP.
7.2.3 Required privileges are approved by authorized personnel.	7.1.4	x	x	Customers are responsible for managing access to all GCP products (GCE, VPC, GCS, etc.) that are included in their CDE. GCP provides various mechanisms for controlling access to the services including IAM for integration with corporate directories and granular access controls to the GCP Management Console.	Customers are responsible for managing access to all GCP products (GCE, VPC, GCS, etc.) that are included in their CDE. GCP provides various mechanisms for controlling access to the services including IAM for integration with corporate directories and granular access controls to the GCP Management Console.	Customers are responsible for managing access to all GCP products (GCE, VPC, GCS, etc.) that are included in their CDE. GCP provides various mechanisms for controlling access to the services including IAM for integration with corporate directories and granular access controls to the GCP Management Console.	Customers are responsible for managing access to all GCP products (GCE, VPC, GCS, etc.) that are included in their CDE. GCP provides various mechanisms for controlling access to the services including IAM for integration with corporate directories and granular access controls to the GCP Management Console.	Google is responsible for implementing access controls in compliance with this requirement for the systems and infrastructure underlying GCP.
7.2.4 All user accounts and related access privileges, including third-party/vendor accounts, are reviewed as follows: • At least once every six months. • To ensure user accounts and access remain appropriate based on job function. • Any inappropriate access is addressed. • Management acknowledges that access remains appropriate.	*New*	x	x	Customers are responsible for managing access to all GCP products (GCE, VPC, GCS, etc.) that are included in their CDE. GCP provides various mechanisms for controlling access to the services including IAM for integration with corporate directories and granular access controls to the GCP Management Console.	Customers are responsible for managing access to all GCP products (GCE, VPC, GCS, etc.) that are included in their CDE. GCP provides various mechanisms for controlling access to the services including IAM for integration with corporate directories and granular access controls to the GCP Management Console.	Customers are responsible for managing access to all GCP products (GCE, VPC, GCS, etc.) that are included in their CDE. GCP provides various mechanisms for controlling access to the services including IAM for integration with corporate directories and granular access controls to the GCP Management Console.	Customers are responsible for managing access to all GCP products (GCE, VPC, GCS, etc.) that are included in their CDE. GCP provides various mechanisms for controlling access to the services including IAM for integration with corporate directories and granular access controls to the GCP Management Console.	Google is responsible for implementing access controls in compliance with this requirement for the systems and infrastructure underlying GCP.
7.2.5 All application and system accounts and related access privileges are assigned and managed as follows: • Based on the least privileges necessary for the operability of the system or application. • Access is limited to the systems, applications, or processes that specifically require their use.	*New*	x	x	Customers are responsible for managing access to all GCP products (GCE, VPC, GCS, etc.) that are included in their CDE. GCP provides various mechanisms for controlling access to the services including IAM for integration with corporate directories and granular access controls to the GCP Management Console.	Customers are responsible for managing access to all GCP products (GCE, VPC, GCS, etc.) that are included in their CDE. GCP provides various mechanisms for controlling access to the services including IAM for integration with corporate directories and granular access controls to the GCP Management Console.	Customers are responsible for managing access to all GCP products (GCE, VPC, GCS, etc.) that are included in their CDE. GCP provides various mechanisms for controlling access to the services including IAM for integration with corporate directories and granular access controls to the GCP Management Console.	Customers are responsible for managing access to all GCP products (GCE, VPC, GCS, etc.) that are included in their CDE. GCP provides various mechanisms for controlling access to the services including IAM for integration with corporate directories and granular access controls to the GCP Management Console.	Google is responsible for implementing access controls in compliance with this requirement for the systems and infrastructure underlying GCP.

PCI DSS 4.0 Requirements	PCI DSS 3.2.1	GCP	Customer	Compute	Networking	Storage	Security & Identity	Google Responsibility Summary
7.2.5.1 All access by application and system accounts and related access privileges are reviewed as follows: • Periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1). • The application/system access remains appropriate for the function being performed. • Any inappropriate access is addressed. • Management acknowledges that access remains appropriate.	*New*		x	Customers are responsible for conducting a targeted risk analysis of their control environment and determining control frequency to meet applicable PCI DSS requirements.	Customers are responsible for conducting a targeted risk analysis of their control environment and determining control frequency to meet applicable PCI DSS requirements.	Customers are responsible for conducting a targeted risk analysis of their control environment and determining control frequency to meet applicable PCI DSS requirements.	Customers are responsible for conducting a targeted risk analysis of their control environment and determining control frequency to meet applicable PCI DSS requirements.	Not Applicable
7.2.6 All user access to query repositories of stored cardholder data is restricted as follows: • Via applications or other programmatic methods, with access and allowed actions based on user roles and least privileges. • Only the responsible administrator(s) can directly access or query repositories of stored CHD.	8.7		x	Customers are responsible for managing the creation of user accounts. This includes access controls to all applications installed by the customer, including databases that may contain CHD.	Not Applicable	Customers are responsible for managing the creation of user accounts. This includes access controls to all applications installed by the customer, including and GCS buckets and potential objects that may contain CHD.	Customers are responsible for managing the creation of user accounts. This includes access controls to all applications installed by the customer, including and GCS buckets and potential objects that may contain CHD.	Not Applicable.
7.3.1 An access control system(s) is in place that restricts access based on a user's need to know and covers all system components.	7.2, 7.2.1	x	x	Customers are responsible for managing access to all GCP products (GCE, VPC, GCS, etc.) that are included in their CDE. GCP provides various mechanisms for controlling access to the services including IAM for integration with corporate directories and granular access controls to the GCP Management Console.	Customers are responsible for managing access to all GCP products (GCE, VPC, GCS, etc.) that are included in their CDE. GCP provides various mechanisms for controlling access to the services including IAM for integration with corporate directories and granular access controls to the GCP Management Console.	Customers are responsible for managing access to all GCP products (GCE, VPC, GCS, etc.) that are included in their CDE. GCP provides various mechanisms for controlling access to the services including IAM for integration with corporate directories and granular access controls to the GCP Management Console.	Customers are responsible for managing access to all GCP products (GCE, VPC, GCS, etc.) that are included in their CDE. GCP provides various mechanisms for controlling access to the services including IAM for integration with corporate directories and granular access controls to the GCP Management Console.	Google is responsible for implementing access controls in compliance with this requirement for the systems and infrastructure underlying GCP.
7.3.2 The access control system(s) is configured to enforce permissions assigned to individuals, applications, and systems based on job classification and function.	7.2.2	x	x	Customers are responsible for managing access to all GCP products (GCE, VPC, GCS, etc.) that are included in their CDE. GCP provides various mechanisms for controlling access to the services including IAM for integration with corporate directories and granular access controls to the GCP Management Console.	Customers are responsible for managing access to all GCP products (GCE, VPC, GCS, etc.) that are included in their CDE. GCP provides various mechanisms for controlling access to the services including IAM for integration with corporate directories and granular access controls to the GCP Management Console.	Customers are responsible for managing access to all GCP products (GCE, VPC, GCS, etc.) that are included in their CDE. GCP provides various mechanisms for controlling access to the services including IAM for integration with corporate directories and granular access controls to the GCP Management Console.	Customers are responsible for managing access to all GCP products (GCE, VPC, GCS, etc.) that are included in their CDE. GCP provides various mechanisms for controlling access to the services including IAM for integration with corporate directories and granular access controls to the GCP Management Console.	Google is responsible for implementing access controls in compliance with this requirement for the systems and infrastructure underlying GCP.
7.3.3 The access control system(s) is set to "deny all" by default.	7.2.3	x	x	Customers are responsible for managing access to all GCP products (GCE, VPC, GCS, etc.) that are included in their CDE. GCP provides various mechanisms for controlling access to the services including IAM for integration with corporate directories and granular access controls to the GCP Management Console.	Customers are responsible for managing access to all GCP products (GCE, VPC, GCS, etc.) that are included in their CDE. GCP provides various mechanisms for controlling access to the services including IAM for integration with corporate directories and granular access controls to the GCP Management Console.	Customers are responsible for managing access to all GCP products (GCE, VPC, GCS, etc.) that are included in their CDE. GCP provides various mechanisms for controlling access to the services including IAM for integration with corporate directories and granular access controls to the GCP Management Console.	Customers are responsible for managing access to all GCP products (GCE, VPC, GCS, etc.) that are included in their CDE. GCP provides various mechanisms for controlling access to the services including IAM for integration with corporate directories and granular access controls to the GCP Management Console.	Google is responsible for implementing access controls in compliance with this requirement for the systems and infrastructure underlying GCP.
Requirement 8: Identify Users and Authenticate Access to System Components								

PCI DSS 4.0 Requirements	PCI DSS 3.2.1	GCP	Customer	Compute	Networking	Storage	Security & Identity	Google Responsibility Summary
8.1.1 All security policies and operational procedures that are identified in Requirement 8 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	8.8		x	Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Not Applicable
8.1.2 Roles and responsibilities for performing activities in Requirement 8 are documented, assigned, and understood.	*New*	x	x	Customers are responsible for documenting and assigning roles and responsibilities for applicable activities. Roles and responsibilities must be understood by assigned individuals.	Customers are responsible for documenting and assigning roles and responsibilities for applicable activities. Roles and responsibilities must be understood by assigned individuals.	Customers are responsible for documenting and assigning roles and responsibilities for applicable activities. Roles and responsibilities must be understood by assigned individuals.	Customers are responsible for documenting and assigning roles and responsibilities for applicable activities. Roles and responsibilities must be understood by assigned individuals.	Google has documented and assigned roles and responsibilities for applicable activities. Roles and responsibilities are understood by assigned individuals.
8.2.1 All users are assigned a unique ID before access to system components or cardholder data is allowed.	8.1.1	x	x	Customers are responsible for managing the creation of user accounts, including GCP accounts. This includes access controls to all in-scope GCP products (GCE, VPC, GCS, etc.) as well as to customer specific applications. Customers may use IAM Workforce Identity Federation to authenticate and authorize its users.	Customers are responsible for managing the creation of user accounts, including GCP accounts. This includes access controls to all in-scope GCP products (GCE, VPC, GCS, etc.) as well as to customer specific applications. Customers may use IAM Workforce Identity Federation to authenticate and authorize its users.	Customers are responsible for managing the creation of user accounts, including GCP accounts. This includes access controls to all in-scope GCP products (GCE, VPC, GCS, etc.) as well as to customer specific applications. Customers may use IAM Workforce Identity Federation to authenticate and authorize its users.	Customers are responsible for managing the creation of user accounts, including GCP accounts. This includes access controls to all in-scope GCP products (GCE, VPC, GCS, etc.) as well as to customer specific applications. Customers may use IAM Workforce Identity Federation to authenticate and authorize its users.	Google is responsible for implementing access controls in compliance with this requirement for the systems and infrastructure underlying GCP.
8.2.2 Group, shared, or generic accounts, or other shared authentication credentials are only used when necessary on an exception basis, and are managed as follows: • Account use is prevented unless needed for an exceptional circumstance. • Use is limited to the time needed for the exceptional circumstance. • Business justification for use is documented. • Use is explicitly approved by management. • Individual user identity is confirmed before access to an account is granted. • Every action taken is attributable to an individual user.	8.5	x	x	Customers are responsible for managing the creation of user accounts, including GCP accounts. This includes access controls to all in-scope GCP products (GCE, VPC, GCS, etc.) as well as to customer specific applications. Customers are not permitted to use any group, generic, or shared accounts as well as passwords to access the CDE.All user accounts must be unique in nature and not shared with any others.	Customers are responsible for managing the creation of user accounts, including GCP accounts. This includes access controls to all in-scope GCP products (GCE, VPC, GCS, etc.) as well as to customer specific applications. Customers are not permitted to use any group, generic, or shared accounts as well as passwords to access the CDE.All user accounts must be unique in nature and not shared with any others.	Customers are responsible for managing the creation of user accounts, including GCP accounts. This includes access controls to all in-scope GCP products (GCE, VPC, GCS, etc.) as well as to customer specific applications. Customers are not permitted to use any group, generic, or shared accounts as well as passwords to access the CDE.All user accounts must be unique in nature and not shared with any others.	Customers are responsible for managing the creation of user accounts, including GCP accounts. This includes access controls to all in-scope GCP products (GCE, VPC, GCS, etc.) as well as to customer specific applications. Customers are not permitted to use any group, generic, or shared accounts as well as passwords to access the CDE.All user accounts must be unique in nature and not shared with any others.	Google is responsible for implementing access controls in compliance with this requirement for the systems and infrastructure underlying GCP.
8.2.3 Additional requirement for service providers only: Service providers with remote access to customer premises use unique authentication factors for each customer premises.	8.5 8.5.1		x	Customers are responsible for managing the creation of user accounts, including GCP accounts. This includes access controls to all in-scope GCP products (GCE, VPC, GCS, etc.) as well as to customer specific applications. If customers are a Service Provider AND have remote access to customer premises they must use a unique authentication credential specific to each customer and not use the same credential for each customer.	Customers are responsible for managing the creation of user accounts, including GCP accounts. This includes access controls to all in-scope GCP products (GCE, VPC, GCS, etc.) as well as to customer specific applications. If customers are a Service Provider AND have remote access to customer premises they must use a unique authentication credential specific to each customer and not use the same credential for each customer.	Customers are responsible for managing the creation of user accounts, including GCP accounts. This includes access controls to all in-scope GCP products (GCE, VPC, GCS, etc.) as well as to customer specific applications. If customers are a Service Provider AND have remote access to customer premises they must use a unique authentication credential specific to each customer and not use the same credential for each customer.	Customers are responsible for managing the creation of user accounts, including GCP accounts. This includes access controls to all in-scope GCP products (GCE, VPC, GCS, etc.) as well as to customer specific applications. If customers are a Service Provider AND have remote access to customer premises they must use a unique authentication credential specific to each customer and not use the same credential for each customer.	Not Applicable. Google does not have remote access to its customer's premises.

PCI DSS 4.0 Requirements	PCI DSS 3.2.1	GCP	Customer	Compute	Networking	Storage	Security & Identity	Google Responsibility Summary
8.2.4 Addition, deletion, and modification of user IDs, authentication factors, and other identifier objects are managed as follows: • Authorized with the appropriate approval. • Implemented with only the privileges specified on the documented approval.	8.1.2	x	x	Customers are responsible for managing the creation, deletion and modification of user accounts, including GCP accounts. This includes access controls to all in-scope GCP products (GCE, VPC, GCS, etc.) as well as to customer specific applications.	Customers are responsible for managing the creation, deletion and modification of user accounts, including GCP accounts. This includes access controls to all in-scope GCP products (GCE, VPC, GCS, etc.) as well as to customer specific applications.	Customers are responsible for managing the creation, deletion and modification of user accounts, including GCP accounts. This includes access controls to all in-scope GCP products (GCE, VPC, GCS, etc.) as well as to customer specific applications.	Customers are responsible for managing the creation, deletion and modification of user accounts, including GCP accounts. This includes access controls to all in-scope GCP products (GCE, VPC, GCS, etc.) as well as to customer specific applications.	Google is responsible for implementing access controls in compliance with this requirement for the systems and infrastructure underlying GCP.
8.2.5 Access for terminated users is immediately revoked.	8.1.3	x	x	Customers are responsible for managing user accounts including termination of accounts for GCP accounts. This includes access controls to all in-scope GCP products (GCE, VPC, GCS, etc.) as well as to customer specific applications.	Customers are responsible for managing user accounts including termination of accounts for GCP accounts. This includes access controls to all in-scope GCP products (GCE, VPC, GCS, etc.) as well as to customer specific applications.	Customers are responsible for managing user accounts including termination of accounts for GCP accounts. This includes access controls to all in-scope GCP products (GCE, VPC, GCS, etc.) as well as to customer specific applications.	Customers are responsible for managing user accounts including termination of accounts for GCP accounts. This includes access controls to all in-scope GCP products (GCE, VPC, GCS, etc.) as well as to customer specific applications.	Google is responsible for implementing access controls in compliance with this requirement for the systems and infrastructure underlying GCP.
8.2.6 Inactive user accounts are removed or disabled within 90 days of inactivity.	8.1.4	x	x	Customers are responsible for managing user accounts including removing/ disabling inactive accounts within 90 days. This includes access controls to all in-scope GCP products (GCE, VPC, GCS, etc.) as well as to customer specific applications.	Customers are responsible for managing user accounts including removing/ disabling inactive accounts within 90 days. This includes access controls to all in-scope GCP products (GCE, VPC, GCS, etc.) as well as to customer specific applications.	Customers are responsible for managing user accounts including removing/ disabling inactive accounts within 90 days. This includes access controls to all in-scope GCP products (GCE, VPC, GCS, etc.) as well as to customer specific applications.	Customers are responsible for managing user accounts including removing/ disabling inactive accounts within 90 days. This includes access controls to all in-scope GCP products (GCE, VPC, GCS, etc.) as well as to customer specific applications.	Google is responsible for implementing access controls in compliance with this requirement for the systems and infrastructure underlying GCP.
8.2.7 Accounts used by third parties to access, support, or maintain system components via remote access are managed as follows: • Enabled only during the time period needed and disabled when not in use. • Use is monitored for unexpected activity.	8.1.5		x	Customers are responsible for managing user accounts and all access to their CDE, including any 3rd party vendor access. This includes access controls to all in-scope GCP products (GCE, VPC, GCS, etc.) as well as to customer specific applications.	Customers are responsible for managing user accounts and all access to their CDE, including any 3rd party vendor access. This includes access controls to all in-scope GCP products (GCE, VPC, GCS, etc.) as well as to customer specific applications.	Customers are responsible for managing user accounts and all access to their CDE, including any 3rd party vendor access. This includes access controls to all in-scope GCP products (GCE, VPC, GCS, etc.) as well as to customer specific applications.	Customers are responsible for managing user accounts and all access to their CDE, including any 3rd party vendor access. This includes access controls to all in-scope GCP products (GCE, VPC, GCS, etc.) as well as to customer specific applications.	Not Applicable. Google does not allow vendor remote access within the in-scope GCP environment.
8.2.8 If a user session has been idle for more than 15 minutes, the user is required to re-authenticate to re-activate the terminal or session.	8.1.8	x	x	Customers are responsible for managing the creation of user accounts, including GCP accounts. This includes access controls to all in-scope GCP products (GCE, VPC, GCS, etc.) as well as to customer specific applications. IAM customers must enforce the 15-minute idle session timeout requirement through either their external identity provider (IdP), or “before” the GCP Management Console.	Customers are responsible for managing the creation of user accounts, including GCP accounts. This includes access controls to all in-scope GCP products (GCE, VPC, GCS, etc.) as well as to customer specific applications. IAM customers must enforce the 15-minute idle session timeout requirement through either their external identity provider (IdP), or “before” the GCP Management Console.	Customers are responsible for managing the creation of user accounts, including GCP accounts. This includes access controls to all in-scope GCP products (GCE, VPC, GCS, etc.) as well as to customer specific applications. IAM customers must enforce the 15-minute idle session timeout requirement through either their external identity provider (IdP), or “before” the GCP Management Console.	Customers are responsible for managing the creation of user accounts, including GCP accounts. This includes access controls to all in-scope GCP products (GCE, VPC, GCS, etc.) as well as to customer specific applications. IAM customers must enforce the 15-minute idle session timeout requirement through either their external identity provider (IdP), or “before” the GCP Management Console.	Google is responsible for implementing access controls in compliance with this requirement for the systems and infrastructure underlying GCP.
8.3.1 All user access to system components for users and administrators is authenticated via at least one of the following authentication factors: • 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 element.	8.2	x	x	Customers are responsible for managing user accounts and all authentication parameters. This includes access, authentication, and authorization controls to all in-scope GCP products (GCE, VPC, GCS, etc.) as well as to customer specific applications. Customers can provide access to GCP products through	Customers are responsible for managing user accounts and all authentication parameters. This includes access, authentication, and authorization controls to all in-scope GCP products (GCE, VPC, GCS, etc.) as well as to customer specific applications. Customers can provide access to GCP products through	Customers are responsible for managing user accounts and all authentication parameters. This includes access, authentication, and authorization controls to all in-scope GCP products (GCE, VPC, GCS, etc.) as well as to customer specific applications. Customers can provide access to GCP products through	Customers are responsible for managing user accounts and all authentication parameters. This includes access, authentication, and authorization controls to all in-scope GCP products (GCE, VPC, GCS, etc.) as well as to customer specific applications. Customers can provide access to GCP products through	Google is responsible for implementing access controls in compliance with this requirement for the systems and infrastructure underlying GCP.

PCI DSS 4.0 Requirements	PCI DSS 3.2.1	GCP	Customer	Compute	Networking	Storage	Security & Identity	Google Responsibility Summary
				identity federation, leverage GCP Directory Services or use their existing third-party identity provider (IdP) to perform account lockout functions.	identity federation, leverage GCP Directory Services or use their existing third-party identity provider (IdP) to perform account lockout functions.	identity federation, leverage GCP Directory Services or use their existing third-party identity provider (IdP) to perform account lockout functions.	identity federation, leverage GCP Directory Services or use their existing third-party identity provider (IdP) to perform account lockout functions.	
8.3.2 Strong cryptography is used to render all authentication factors unreadable during transmission and storage on all system components.	8.2.1	x	x	Customers are responsible for the creation of accounts using their desired authentication mechanisms. For accounts managed by IAM, passwords are rendered unreadable in storage and transmission and fully managed by GCP. Customers connecting IAM to the corporate directory are responsible for rendering credentials unreadable in storage and in transit.	Customers are responsible for the creation of accounts using their desired authentication mechanisms. For accounts managed by IAM, passwords are rendered unreadable in storage and transmission and fully managed by GCP. Customers connecting IAM to the corporate directory are responsible for rendering credentials unreadable in storage and in transit.	Customers are responsible for the creation of accounts using their desired authentication mechanisms. For accounts managed by IAM, passwords are rendered unreadable in storage and transmission and fully managed by GCP. Customers connecting IAM to the corporate directory are responsible for rendering credentials unreadable in storage and in transit.	Customers are responsible for the creation of accounts using their desired authentication mechanisms. For accounts managed by IAM, passwords are rendered unreadable in storage and transmission and fully managed by GCP. Customers connecting IAM to the corporate directory are responsible for rendering credentials unreadable in storage and in transit.	Google is responsible for implementing access controls in compliance with this requirement for the systems and infrastructure underlying GCP.
8.3.3 User identity is verified before modifying any authentication factor.	8.2.2	x	x	Customers are responsible for managing the creation of user accounts, including GCP accounts. This includes access controls to all in-scope GCP products (GCE, VPC, GCS, etc.) as well as to customer specific applications. Customers are required to have a process in place to verify user identity prior to performing any password resets, provisioning new tokens or generating new keys.	Customers are responsible for managing the creation of user accounts, including GCP accounts. This includes access controls to all in-scope GCP products (GCE, VPC, GCS, etc.) as well as to customer specific applications. Customers are required to have a process in place to verify user identity prior to performing any password resets, provisioning new tokens or generating new keys.	Customers are responsible for managing the creation of user accounts, including GCP accounts. This includes access controls to all in-scope GCP products (GCE, VPC, GCS, etc.) as well as to customer specific applications. Customers are required to have a process in place to verify user identity prior to performing any password resets, provisioning new tokens or generating new keys.	Customers are responsible for managing the creation of user accounts, including GCP accounts. This includes access controls to all in-scope GCP products (GCE, VPC, GCS, etc.) as well as to customer specific applications. Customers are required to have a process in place to verify user identity prior to performing any password resets, provisioning new tokens or generating new keys.	Google is responsible for implementing access controls in compliance with this requirement for the systems and infrastructure underlying GCP.
8.3.4 Invalid authentication attempts are limited by: • Locking out the user ID after not more than 10 attempts. • Setting the lockout duration to a minimum of 30 minutes or until the user's identity is confirmed.	8.1.6, 8.1.7	x	x	Customers are responsible for managing user accounts and all authentication parameters. This includes access, authentication, and authorization controls to all in-scope GCP products (GCE, VPC, GCS, etc.) as well as to customer specific applications. Customers can provide access to GCP products through identity federation, leverage GCP Directory Services or use their existing third-party identity provider (IdP) to perform account lockout functions.	Customers are responsible for managing user accounts and all authentication parameters. This includes access, authentication, and authorization controls to all in-scope GCP products (GCE, VPC, GCS, etc.) as well as to customer specific applications. Customers can provide access to GCP products through identity federation, leverage GCP Directory Services or use their existing third-party identity provider (IdP) to perform account lockout functions.	Customers are responsible for managing user accounts and all authentication parameters. This includes access, authentication, and authorization controls to all in-scope GCP products (GCE, VPC, GCS, etc.) as well as to customer specific applications. Customers can provide access to GCP products through identity federation, leverage GCP Directory Services or use their existing third-party identity provider (IdP) to perform account lockout functions.	Customers are responsible for managing user accounts and all authentication parameters. This includes access, authentication, and authorization controls to all in-scope GCP products (GCE, VPC, GCS, etc.) as well as to customer specific applications. Customers can provide access to GCP products through identity federation, leverage GCP Directory Services or use their existing third-party identity provider (IdP) to perform account lockout functions.	Google is responsible for implementing access controls in compliance with this requirement 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 ten invalid access attempts.
8.3.5 If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they are set and reset for each user as follows: • Set to a unique value for first-time use and upon reset. • Forced to be changed immediately after the first use.	8.2.6	x	x	Customers are responsible for the creation of accounts using their desired authentication mechanisms and enforcing password policies requiring that any first time use or reset passwords must be changed immediately. This includes IAM passwords or federated passwords to customer corporate directory service/s.	Customers are responsible for the creation of accounts using their desired authentication mechanisms and enforcing password policies requiring that any first time use or reset passwords must be changed immediately. This includes IAM passwords or federated passwords to customer corporate directory service/s.	Customers are responsible for the creation of accounts using their desired authentication mechanisms and enforcing password policies requiring that any first time use or reset passwords must be changed immediately. This includes IAM passwords or federated passwords to customer corporate directory service/s.	Customers are responsible for the creation of accounts using their desired authentication mechanisms and enforcing password policies requiring that any first time use or reset passwords must be changed immediately. This includes IAM passwords or federated passwords to customer corporate directory service/s.	Google is responsible for implementing access controls in compliance with this requirement for the systems and infrastructure underlying GCP.

PCI DSS 4.0 Requirements	PCI DSS 3.2.1	GCP	Customer	Compute	Networking	Storage	Security & Identity	Google Responsibility Summary
8.3.6 If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they meet the following minimum level of complexity: • A minimum length of 12 characters (or IF the system does not support 12 characters, a minimum length of eight characters). • Contain both numeric and alphabetic characters.	8.2.3	x	x	Customers are responsible for the creation of accounts using their desired authentication mechanisms. For accounts managed by IAM, password policies enforce minimum length and complexity requirements in accordance with PCI DSS requirements. Customers can also integrate Multi-Factor Authentication provided by GCP or connect to a corporate directory service.	Customers are responsible for the creation of accounts using their desired authentication mechanisms. For accounts managed by IAM, password policies enforce minimum length and complexity requirements in accordance with PCI DSS requirements. Customers can also integrate Multi-Factor Authentication provided by GCP or connect to a corporate directory service.	Customers are responsible for the creation of accounts using their desired authentication mechanisms. For accounts managed by IAM, password policies enforce minimum length and complexity requirements in accordance with PCI DSS requirements. Customers can also integrate Multi-Factor Authentication provided by GCP or connect to a corporate directory service.	Customers are responsible for the creation of accounts using their desired authentication mechanisms. For accounts managed by IAM, password policies enforce minimum length and complexity requirements in accordance with PCI DSS requirements. Customers can also integrate Multi-Factor Authentication provided by GCP or connect to a corporate directory service.	Google is responsible for implementing access controls in compliance with this requirement for the systems and infrastructure underlying GCP.
8.3.7 Individuals are not allowed to submit a new password/passphrase that is the same as any of the last four passwords/passphrases used.	8.2.5	x	x	Customers are responsible for the creation of accounts using their desired authentication mechanisms. For accounts managed by IAM, password policies enforce password history, which the customer must enforce to no fewer than the last 4 used. Customers can also integrate Multi-Factor Authentication provided by GCP or connect to a corporate directory service.	Customers are responsible for the creation of accounts using their desired authentication mechanisms. For accounts managed by IAM, password policies enforce password history, which the customer must enforce to no fewer than the last 4 used. Customers can also integrate Multi-Factor Authentication provided by GCP or connect to a corporate directory service.	Customers are responsible for the creation of accounts using their desired authentication mechanisms. For accounts managed by IAM, password policies enforce password history, which the customer must enforce to no fewer than the last 4 used. Customers can also integrate Multi-Factor Authentication provided by GCP or connect to a corporate directory service.	Customers are responsible for the creation of accounts using their desired authentication mechanisms. For accounts managed by IAM, password policies enforce password history, which the customer must enforce to no fewer than the last 4 used. Customers can also integrate Multi-Factor Authentication provided by GCP or connect to a corporate directory service.	Google is responsible for implementing access controls in compliance with this requirement for the systems and infrastructure underlying GCP.
8.3.8 Authentication policies and procedures are documented and communicated to all users including: • Guidance on selecting strong authentication factors. • Guidance for how users should protect their authentication factors. • Instructions not to reuse previously used passwords/passphrases. • Instructions to change passwords/passphrases if there is any suspicion or knowledge that the password/passphrases have been compromised and how to report the incident.	8.4	x	x	Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Google is responsible for implementing access controls in compliance with this requirement for the systems and infrastructure underlying GCP.
8.3.9 If passwords/passphrases are used as the only authentication factor for user access (i.e., in any single-factor authentication implementation) then either: • Passwords/passphrases are changed at least once every 90 days, OR • The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly.	8.2.4	x	x	Customers are responsible for the creation of accounts using their desired authentication mechanisms. For accounts managed by IAM, password policies enforce password rotation, which the customer must enforce to no greater than every 90 days. Customers can also integrate Multi-Factor Authentication provided by GCP or connect to a corporate directory service.	Customers are responsible for the creation of accounts using their desired authentication mechanisms. For accounts managed by IAM, password policies enforce password rotation, which the customer must enforce to no greater than every 90 days. Customers can also integrate Multi-Factor Authentication provided by GCP or connect to a corporate directory service.	Customers are responsible for the creation of accounts using their desired authentication mechanisms. For accounts managed by IAM, password policies enforce password rotation, which the customer must enforce to no greater than every 90 days. Customers can also integrate Multi-Factor Authentication provided by GCP or connect to a corporate directory service.	Customers are responsible for the creation of accounts using their desired authentication mechanisms. For accounts managed by IAM, password policies enforce password rotation, which the customer must enforce to no greater than every 90 days. Customers can also integrate Multi-Factor Authentication provided by GCP or connect to a corporate directory service.	Google is responsible for implementing access controls in compliance with this requirement for the systems and infrastructure underlying GCP.

PCI DSS 4.0 Requirements	PCI DSS 3.2.1	GCP	Customer	Compute	Networking	Storage	Security & Identity	Google Responsibility Summary
8.3.10 Additional requirement for service providers only: If passwords/passphrases are used as the only authentication factor for customer user access to cardholder data (i.e., in any single- factor authentication implementation), then guidance is provided to customer users including: • Guidance for customers to change their user passwords/passphrases periodically. • Guidance as to when, and under what circumstances, passwords/passphrases are to be changed.	8.2.4.b		x	Customers are responsible for the creation of accounts using their desired authentication mechanisms. For accounts managed by IAM, password policies enforce password rotation, which the customer must enforce to no greater than every 90 days. Customers can also integrate Multi-Factor Authentication provided by GCP or connect to a corporate directory service.	Customers are responsible for the creation of accounts using their desired authentication mechanisms. For accounts managed by IAM, password policies enforce password rotation, which the customer must enforce to no greater than every 90 days. Customers can also integrate Multi-Factor Authentication provided by GCP or connect to a corporate directory service.	Customers are responsible for the creation of accounts using their desired authentication mechanisms. For accounts managed by IAM, password policies enforce password rotation, which the customer must enforce to no greater than every 90 days. Customers can also integrate Multi-Factor Authentication provided by GCP or connect to a corporate directory service.	Customers are responsible for the creation of accounts using their desired authentication mechanisms. For accounts managed by IAM, password policies enforce password rotation, which the customer must enforce to no greater than every 90 days. Customers can also integrate Multi-Factor Authentication provided by GCP or connect to a corporate directory service.	Not Applicable.
8.3.10.1 Additional requirement for service providers only: If passwords/passphrases are used as the only authentication factor for customer user access (i.e., in any single-factor authentication implementation) then either: • Passwords/passphrases are changed at least once every 90 days, OR • The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly.	*New*		x	Customers are responsible for the creation of accounts using their desired authentication mechanisms. For accounts managed by IAM, password policies enforce password rotation, which the customer must enforce to no greater than every 90 days. Customers can also integrate Multi-Factor Authentication provided by GCP or connect to a corporate directory service.	Customers are responsible for the creation of accounts using their desired authentication mechanisms. For accounts managed by IAM, password policies enforce password rotation, which the customer must enforce to no greater than every 90 days. Customers can also integrate Multi-Factor Authentication provided by GCP or connect to a corporate directory service.	Customers are responsible for the creation of accounts using their desired authentication mechanisms. For accounts managed by IAM, password policies enforce password rotation, which the customer must enforce to no greater than every 90 days. Customers can also integrate Multi-Factor Authentication provided by GCP or connect to a corporate directory service.	Customers are responsible for the creation of accounts using their desired authentication mechanisms. For accounts managed by IAM, password policies enforce password rotation, which the customer must enforce to no greater than every 90 days. Customers can also integrate Multi-Factor Authentication provided by GCP or connect to a corporate directory service.	Not Applicable.
8.3.11 Where authentication factors such as physical or logical security tokens, smart cards, or certificates are used: • Factors are assigned to an individual user and not shared among multiple users. • Physical and/or logical controls ensure only the intended user can use that factor to gain access.	8.6	x	x	Customers are responsible for the authentication mechanisms to the management consoles and APIs for managing their GCP Projects. GCP provides an MFA solution, Google Authenticator, to support customers meeting the requirement for Multi-Factor authentication. Customers may also select any MFA IdP they choose to meet their needs, but it must be implemented and enforced for all GCP products in-scope.	Customers are responsible for the authentication mechanisms to the management consoles and APIs for managing their GCP Projects. GCP provides an MFA solution, Google Authenticator, to support customers meeting the requirement for Multi-Factor authentication. Customers may also select any MFA IdP they choose to meet their needs, but it must be implemented and enforced for all GCP products in-scope.	Customers are responsible for the authentication mechanisms to the management consoles and APIs for managing their GCP Projects. GCP provides an MFA solution, Google Authenticator, to support customers meeting the requirement for Multi-Factor authentication. Customers may also select any MFA IdP they choose to meet their needs, but it must be implemented and enforced for all GCP products in-scope.	Customers are responsible for the authentication mechanisms to the management consoles and APIs for managing their GCP Projects. GCP provides an MFA solution, Google Authenticator, to support customers meeting the requirement for Multi-Factor authentication. Customers may also select any MFA IdP they choose to meet their needs, but it must be implemented and enforced for all GCP products in-scope.	Google is responsible for implementing access controls in compliance with this requirement for the systems and infrastructure underlying GCP.
8.4.1 MFA is implemented for all non-console access into the CDE for personnel with administrative access.	8.3.1	x	x	Customers are responsible for the authentication mechanisms to the management consoles and APIs for managing their GCP Projects. GCP provides an MFA solution, Google Authenticator, to support customers meeting the requirement for Multi-Factor authentication. Customers may also select any MFA IdP they choose to meet their needs, but it must be implemented and enforced for all GCP products in-scope.	Customers are responsible for the authentication mechanisms to the management consoles and APIs for managing their GCP Projects. GCP provides an MFA solution, Google Authenticator, to support customers meeting the requirement for Multi-Factor authentication. Customers may also select any MFA IdP they choose to meet their needs, but it must be implemented and enforced for all GCP products in-scope.	Customers are responsible for the authentication mechanisms to the management consoles and APIs for managing their GCP Projects. GCP provides an MFA solution, Google Authenticator, to support customers meeting the requirement for Multi-Factor authentication. Customers may also select any MFA IdP they choose to meet their needs, but it must be implemented and enforced for all GCP products in-scope.	Customers are responsible for the authentication mechanisms to the management consoles and APIs for managing their GCP Projects. GCP provides an MFA solution, Google Authenticator, to support customers meeting the requirement for Multi-Factor authentication. Customers may also select any MFA IdP they choose to meet their needs, but it must be implemented and enforced for all GCP products in-scope.	Google is responsible for implementing access controls in compliance with this requirement for the systems and infrastructure underlying GCP.

PCI DSS 4.0 Requirements	PCI DSS 3.2.1	GCP	Customer	Compute	Networking	Storage	Security & Identity	Google Responsibility Summary
8.4.2 MFA is implemented for all access into the CDE.	*New*	x	x	Customers are responsible for the authentication mechanisms to the management consoles and APIs for managing their GCP Projects. GCP provides an MFA solution, Google Authenticator, to support customers meeting the requirement for Multi-Factor authentication. Customers may also select any MFA IdP they choose to meet their needs, but it must be implemented and enforced for all GCP products in-scope.	Customers are responsible for the authentication mechanisms to the management consoles and APIs for managing their GCP Projects. GCP provides an MFA solution, Google Authenticator, to support customers meeting the requirement for Multi-Factor authentication. Customers may also select any MFA IdP they choose to meet their needs, but it must be implemented and enforced for all GCP products in-scope.	Customers are responsible for the authentication mechanisms to the management consoles and APIs for managing their GCP Projects. GCP provides an MFA solution, Google Authenticator, to support customers meeting the requirement for Multi-Factor authentication. Customers may also select any MFA IdP they choose to meet their needs, but it must be implemented and enforced for all GCP products in-scope.	Customers are responsible for the authentication mechanisms to the management consoles and APIs for managing their GCP Projects. GCP provides an MFA solution, Google Authenticator, to support customers meeting the requirement for Multi-Factor authentication. Customers may also select any MFA IdP they choose to meet their needs, but it must be implemented and enforced for all GCP products in-scope.	Google is responsible for implementing access controls in compliance with this requirement for the systems and infrastructure underlying GCP.
8.4.3 MFA is implemented for all remote network access originating from outside the entity's network that could access or impact the CDE as follows: • All remote access by all personnel, both users and administrators, originating from outside the entity's network. • All remote access by third parties and vendors.	8.3.2	x	x	Customers are responsible for the authentication mechanisms to the management consoles and APIs for managing their GCP Projects. GCP provides an MFA solution, Google Authenticator, to support customers meeting the requirement for Multi-Factor authentication. Customers may also select any MFA IdP they choose to meet their needs, but it must be implemented and enforced for all GCP products in-scope.	Customers are responsible for the authentication mechanisms to the management consoles and APIs for managing their GCP Projects. GCP provides an MFA solution, Google Authenticator, to support customers meeting the requirement for Multi-Factor authentication. Customers may also select any MFA IdP they choose to meet their needs, but it must be implemented and enforced for all GCP products in-scope.	Customers are responsible for the authentication mechanisms to the management consoles and APIs for managing their GCP Projects. GCP provides an MFA solution, Google Authenticator, to support customers meeting the requirement for Multi-Factor authentication. Customers may also select any MFA IdP they choose to meet their needs, but it must be implemented and enforced for all GCP products in-scope.	Customers are responsible for the authentication mechanisms to the management consoles and APIs for managing their GCP Projects. GCP provides an MFA solution, Google Authenticator, to support customers meeting the requirement for Multi-Factor authentication. Customers may also select any MFA IdP they choose to meet their needs, but it must be implemented and enforced for all GCP products in-scope.	Google is responsible for implementing access controls in compliance with this requirement for the systems and infrastructure underlying GCP.
8.5.1 MFA systems are implemented as follows: • The MFA system is not susceptible to replay attacks. • MFA systems cannot be bypassed by any users, including administrative users unless specifically documented, and authorized by management on an exception basis, for a limited time period. • At least two different types of authentication factors are used. • Success of all authentication factors is required before access is granted.	*New*	x	x	Customers are responsible for the authentication mechanisms to the management consoles and APIs for managing their GCP Projects. GCP provides an MFA solution, Google Authenticator, to support customers meeting the requirement for Multi-Factor authentication. Customers may also select any MFA IdP they choose to meet their needs, but it must be implemented and enforced for all GCP products in-scope.	Customers are responsible for the authentication mechanisms to the management consoles and APIs for managing their GCP Projects. GCP provides an MFA solution, Google Authenticator, to support customers meeting the requirement for Multi-Factor authentication. Customers may also select any MFA IdP they choose to meet their needs, but it must be implemented and enforced for all GCP products in-scope.	Customers are responsible for the authentication mechanisms to the management consoles and APIs for managing their GCP Projects. GCP provides an MFA solution, Google Authenticator, to support customers meeting the requirement for Multi-Factor authentication. Customers may also select any MFA IdP they choose to meet their needs, but it must be implemented and enforced for all GCP products in-scope.	Customers are responsible for the authentication mechanisms to the management consoles and APIs for managing their GCP Projects. GCP provides an MFA solution, Google Authenticator, to support customers meeting the requirement for Multi-Factor authentication. Customers may also select any MFA IdP they choose to meet their needs, but it must be implemented and enforced for all GCP products in-scope.	Google is responsible for implementing access controls in compliance with this requirement for the systems and infrastructure underlying GCP.
8.6.1 If accounts used by systems or applications can be used for interactive login, they are managed as follows: • Interactive use is prevented unless needed for an exceptional circumstance. • Interactive use is limited to the time needed for the exceptional circumstance. • Business justification for interactive use is documented. • Interactive use is explicitly approved by management. • Individual user identity is confirmed before access to account is granted. • Every action taken is attributable to an individual user.	*New*	x	x	Customers are responsible for managing user accounts and all authentication parameters. This includes access, authentication, and authorization controls to all in-scope GCP products (GCE, VPC, GCS, etc.) as well as to customer specific applications. Customers can provide access to GCP products through identity federation, leverage GCP Directory Services or use their existing	Customers are responsible for managing user accounts and all authentication parameters. This includes access, authentication, and authorization controls to all in-scope GCP products (GCE, VPC, GCS, etc.) as well as to customer specific applications. Customers can provide access to GCP products through identity federation, leverage GCP Directory Services or use their existing	Customers are responsible for managing user accounts and all authentication parameters. This includes access, authentication, and authorization controls to all in-scope GCP products (GCE, VPC, GCS, etc.) as well as to customer specific applications. Customers can provide access to GCP products through identity federation, leverage GCP Directory Services or use their existing	Customers are responsible for managing user accounts and all authentication parameters. This includes access, authentication, and authorization controls to all in-scope GCP products (GCE, VPC, GCS, etc.) as well as to customer specific applications. Customers can provide access to GCP products through identity federation, leverage GCP Directory Services or use their existing	Google is responsible for implementing access controls in compliance with this requirement for the systems and infrastructure underlying GCP.

PCI DSS 4.0 Requirements	PCI DSS 3.2.1	GCP	Customer	Compute	Networking	Storage	Security & Identity	Google Responsibility Summary
				third-party identity provider (IdP) to perform account lockout functions.	third-party identity provider (IdP) to perform account lockout functions.	third-party identity provider (IdP) to perform account lockout functions.	third-party identity provider (IdP) to perform account lockout functions.	
8.6.2 Passwords/passphrases for any application and system accounts that can be used for interactive login are not hard coded in scripts, configuration/property files, or bespoke and custom source code.	*New*	x	x	Customers are responsible for managing user accounts and all authentication parameters. This includes access, authentication, and authorization controls to all in-scope GCP products (GCE, VPC, GCS, etc.) as well as to customer specific applications. Customers can provide access to GCP products through identity federation, leverage GCP Directory Services or use their existing third-party identity provider (IdP) to perform account lockout functions.	Customers are responsible for managing user accounts and all authentication parameters. This includes access, authentication, and authorization controls to all in-scope GCP products (GCE, VPC, GCS, etc.) as well as to customer specific applications. Customers can provide access to GCP products through identity federation, leverage GCP Directory Services or use their existing third-party identity provider (IdP) to perform account lockout functions.	Customers are responsible for managing user accounts and all authentication parameters. This includes access, authentication, and authorization controls to all in-scope GCP products (GCE, VPC, GCS, etc.) as well as to customer specific applications. Customers can provide access to GCP products through identity federation, leverage GCP Directory Services or use their existing third-party identity provider (IdP) to perform account lockout functions.	Customers are responsible for managing user accounts and all authentication parameters. This includes access, authentication, and authorization controls to all in-scope GCP products (GCE, VPC, GCS, etc.) as well as to customer specific applications. Customers can provide access to GCP products through identity federation, leverage GCP Directory Services or use their existing third-party identity provider (IdP) to perform account lockout functions. Customers may use Cloud DLP to identify instances of passwords and other sensitive credentials being hardcoded into scripts, configuration/property files, or bespoke and customer source code.	Google is responsible for implementing access controls in compliance with this requirement for the systems and infrastructure underlying GCP.
8.6.3 Passwords/passphrases for any application and system accounts are protected against misuse as follows: • Passwords/passphrases are changed periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1) and upon suspicion or confirmation of compromise. • Passwords/passphrases are constructed with sufficient complexity appropriate for how frequently the entity changes the passwords/passphrases.	*New*		x	Customers are responsible for conducting a targeted risk analysis of their control environment and determining control frequency to meet applicable PCI DSS requirements.	Customers are responsible for conducting a targeted risk analysis of their control environment and determining control frequency to meet applicable PCI DSS requirements.	Customers are responsible for conducting a targeted risk analysis of their control environment and determining control frequency to meet applicable PCI DSS requirements.	Customers are responsible for conducting a targeted risk analysis of their control environment and determining control frequency to meet applicable PCI DSS requirements. Customers may use Security Command Center Premium to validate that credentials are appropriately complex to withstand 'ncrack' brute force methods.	Not Applicable.
Requirement 9: Restrict Physical Access to Cardholder Data								
9.1.1 All security policies and operational procedures that are identified in Requirement 9 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	9.10		x	Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Not Applicable
9.1.2 Roles and responsibilities for performing activities in Requirement 9 are documented, assigned, and understood.	*New*	x	x	Customers are responsible for documenting and assigning roles and responsibilities for applicable activities. Roles and responsibilities must be understood by assigned individuals.	Customers are responsible for documenting and assigning roles and responsibilities for applicable activities. Roles and responsibilities must be understood by assigned individuals.	Customers are responsible for documenting and assigning roles and responsibilities for applicable activities. Roles and responsibilities must be understood by assigned individuals.	Customers are responsible for documenting and assigning roles and responsibilities for applicable activities. Roles and responsibilities must be understood by assigned individuals.	Google has documented and assigned roles and responsibilities for applicable activities. Roles and responsibilities are understood by assigned individuals.
9.2.1 Appropriate facility entry controls are in place to restrict physical access to systems in the CDE.	9.1	x		Not Applicable	Not Applicable	Not Applicable	Not Applicable	Google maintains the physical security and media handling controls

PCI DSS 4.0 Requirements	PCI DSS 3.2.1	GCP	Customer	Compute	Networking	Storage	Security & Identity	Google Responsibility Summary
								for data centers and colocation facilities that host GCP Products.
9.2.1.1 Individual physical access to sensitive areas within the CDE is monitored with either video cameras or physical access control mechanisms (or both) as follows: • Entry and exit points to/from sensitive areas within the CDE are monitored. • Monitoring devices or mechanisms are protected from tampering or disabling. • Collected data is reviewed and correlated with other entries. • Collected data is stored for at least three months, unless otherwise restricted by law.	9.1.1	x		Not Applicable	Not Applicable	Not Applicable	Not Applicable	Google maintains the physical security and media handling controls for data centers and colocation facilities that host GCP Products.
9.2.2 Physical and/or logical controls are implemented to restrict use of publicly accessible network jacks within the facility.	9.1.2	x		Not Applicable	Not Applicable	Not Applicable	Not Applicable	Google maintains the physical security and media handling controls for data centers and colocation facilities that host GCP Products.
9.2.3 Physical access to wireless access points, gateways, networking/communications hardware, and telecommunication lines within the facility is restricted.	9.1.3	x		Not Applicable	Not Applicable	Not Applicable	Not Applicable	Google maintains the physical security and media handling controls for data centers and colocation facilities that host GCP Products.
9.2.4 Access to consoles in sensitive areas is restricted via locking when not in use.	9.1	x		Not Applicable	Not Applicable	Not Applicable	Not Applicable	Google maintains the physical security and media handling controls for data centers and colocation facilities that host GCP Products.
9.3.1 Procedures are implemented for authorizing and managing physical access of personnel to the CDE, including: • Identifying personnel. • Managing changes to an individual's physical access requirements. • Revoking or terminating personnel identification. • Limiting access to the identification process or system to authorized personnel.	9.2	x		Not Applicable	Not Applicable	Not Applicable	Not Applicable	Google maintains the physical security and media handling controls for data centers and colocation facilities that host GCP Products.
9.3.1.1 Physical access to sensitive areas within the CDE for personnel is controlled as follows: • Access is authorized and based on individual job function. • Access is revoked immediately upon termination. • All physical access mechanisms, such as keys, access cards, etc., are returned or disabled upon termination.	9.3	x		Not Applicable	Not Applicable	Not Applicable	Not Applicable	Google maintains the physical security and media handling controls for data centers and colocation facilities that host GCP Products.
9.3.2 Procedures are implemented for authorizing and managing visitor access to the CDE, including: • Visitors are authorized before entering. • Visitors are escorted at all times. • Visitors are clearly identified and given a badge or other identification that expires. • Visitor badges or other identification visibly distinguishes visitors from personnel.	9.2, 9.4, 9.4.1, 9.4.2	x		Not Applicable	Not Applicable	Not Applicable	Not Applicable	Google maintains the physical security and media handling controls for data centers and colocation facilities that host GCP Products.

PCI DSS 4.0 Requirements	PCI DSS 3.2.1	GCP	Customer	Compute	Networking	Storage	Security & Identity	Google Responsibility Summary
9.3.3 Visitor badges or identification are surrendered or deactivated before visitors leave the facility or at the date of expiration.	9.4.3	x		Not Applicable	Not Applicable	Not Applicable	Not Applicable	Google maintains the physical security and media handling controls for data centers and colocation facilities that host GCP Products.
9.3.4 A visitor log is used to maintain a physical record of visitor activity within the facility and within sensitive areas, including: • The visitor's name and the organization represented. • The date and time of the visit. • The name of the personnel authorizing physical access. • Retaining the log for at least three months, unless otherwise restricted by law.	9.4.4	x		Not Applicable	Not Applicable	Not Applicable	Not Applicable	Google maintains the physical security and media handling controls for data centers and colocation facilities that host GCP Products.
9.4.1 All media with cardholder data is physically secured.	9.5	x	x	Customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	Customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	Customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	Customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	Google maintains the physical security and media handling controls for data centers and colocation facilities that host GCP Products. Google does not store customer data on removable media.
9.4.1.1 Offline media backups with cardholder data are stored in a secure location.	9.5.1	x	x	Customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	Customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	Customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	Customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	Google maintains the physical security and media handling controls for data centers and colocation facilities that host GCP Products. Google does not store customer data on removable media.
9.4.1.2 The security of the offline media backup location(s) with cardholder data is reviewed at least once every 12 months.	9.5.1	x	x	Customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	Customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	Customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	Customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	Google maintains the physical security and media handling controls for data centers and colocation facilities that host GCP Products. Google does not store customer data on removable media.
9.4.2 All media with cardholder data is classified in accordance with the sensitivity of the data.	9.6, 9.6.1	x	x	Customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	Customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	Customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	Customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	Google maintains the physical security and media handling controls for data centers and colocation facilities that host GCP Products. Google does not store customer data on removable media.
9.4.3 Media with cardholder data sent outside the facility is secured as follows: • Media sent outside the facility is logged. • Media is sent by secured courier or other delivery method that can be accurately tracked. • Offsite tracking logs include details about media location.	9.6, 9.6.2	x	x	Customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	Customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	Customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	Customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	Google maintains the physical security and media handling controls for data centers and colocation facilities that host GCP Products. Google does not store customer data on removable media.
9.4.4 Management approves all media with cardholder data that is moved outside the facility (including when media is distributed to individuals).	9.6, 9.6.3	x	x	Customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	Customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	Customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	Customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	Google maintains the physical security and media handling controls for data centers and colocation facilities that host GCP Products. Google does not store customer data on removable media.

PCI DSS 4.0 Requirements	PCI DSS 3.2.1	GCP	Customer	Compute	Networking	Storage	Security & Identity	Google Responsibility Summary
9.4.5 Inventory logs of all electronic media with cardholder data are maintained.	9.7	x	x	Customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	Customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	Customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	Customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	Google maintains the physical security and media handling controls for data centers and colocation facilities that host GCP Products. Google does not store customer data on removable media.
9.4.5.1 Inventories of electronic media with cardholder data are conducted at least once every 12 months.	9.7.1	x	x	Customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	Customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	Customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	Customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	Google maintains the physical security and media handling controls for data centers and colocation facilities that host GCP Products. Google does not store customer data on removable media.
9.4.6 Hard-copy materials with cardholder data are destroyed when no longer needed for business or legal reasons, as follows: • Materials are cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed. • Materials are stored in secure storage containers prior to destruction.	9.8, 9.8.1	x	x	Customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	Customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	Customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	Customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	Google maintains the physical security and media handling controls for data centers and colocation facilities that host GCP Products. Google does not store customer data on removable media.
9.4.7 Electronic media with cardholder data is destroyed when no longer needed for business or legal reasons via one of the following: • The electronic media is destroyed. • The cardholder data is rendered unrecoverable so that it cannot be reconstructed.	9.8, 9.8.2	x	x	Customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	Customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	Customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	Customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	Google maintains the physical security and media handling controls for data centers and colocation facilities that host GCP Products. Google does not store customer data on removable media.
9.5.1 POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: • Maintaining a list of POI devices. • Periodically inspecting POI devices to look for tampering or unauthorized substitution. • Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices.	9.9		x	Customers are responsible for all devices that capture cardholder data via direct physical interaction with the payment card.	Customers are responsible for all devices that capture cardholder data via direct physical interaction with the payment card.	Customers are responsible for all devices that capture cardholder data via direct physical interaction with the payment card.	Customers are responsible for all devices that capture cardholder data via direct physical interaction with the payment card.	Not Applicable
9.5.1.1 An up-to-date list of POI devices is maintained, including: • Make and model of the device. • Location of device. • Device serial number or other methods of unique identification.	9.9.1		x	Customers are responsible for all devices that capture cardholder data via direct physical interaction with the payment card.	Customers are responsible for all devices that capture cardholder data via direct physical interaction with the payment card.	Customers are responsible for all devices that capture cardholder data via direct physical interaction with the payment card.	Customers are responsible for all devices that capture cardholder data via direct physical interaction with the payment card.	Not Applicable
9.5.1.2 POI device surfaces are periodically inspected to detect tampering and unauthorized substitution.	9.9.2		x	Customers are responsible for all devices that capture cardholder data via direct physical interaction with the payment card.	Customers are responsible for all devices that capture cardholder data via direct physical interaction with the payment card.	Customers are responsible for all devices that capture cardholder data via direct physical interaction with the payment card.	Customers are responsible for all devices that capture cardholder data via direct physical interaction with the payment card.	Not Applicable
9.5.1.2.1 The frequency of periodic POI device inspections and the type of inspections performed is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.	*New*		x	Customers are responsible for conducting a targeted risk analysis of their control environment and	Customers are responsible for conducting a targeted risk analysis of their control environment and	Customers are responsible for conducting a targeted risk analysis of their control environment and	Customers are responsible for conducting a targeted risk analysis of their control environment and	Not Applicable

PCI DSS 4.0 Requirements	PCI DSS 3.2.1	GCP	Customer	Compute	Networking	Storage	Security & Identity	Google Responsibility Summary
				determining control frequency to meet applicable PCI DSS requirements.	determining control frequency to meet applicable PCI DSS requirements.	determining control frequency to meet applicable PCI DSS requirements.	determining control frequency to meet applicable PCI DSS requirements.	
9.5.1.3 Training is provided for personnel in POI environments to be aware of attempted tampering or replacement of POI devices, and includes: • Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, before granting them access to modify or troubleshoot devices. • Procedures to ensure devices are not installed, replaced, or returned without verification. • Being aware of suspicious behavior around devices. • Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel.	9.9.3		x	Customers are responsible for all devices that capture cardholder data via direct physical interaction with the payment card.	Customers are responsible for all devices that capture cardholder data via direct physical interaction with the payment card.	Customers are responsible for all devices that capture cardholder data via direct physical interaction with the payment card.	Customers are responsible for all devices that capture cardholder data via direct physical interaction with the payment card.	Not Applicable
Requirement 10: Log and Monitor All Access to System Components and Cardholder Data								
10.1.1 All security policies and operational procedures that are identified in Requirement 10 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	10.9		x	Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Not Applicable
10.1.2 Roles and responsibilities for performing activities in Requirement 10 are documented, assigned, and understood.	*New*	x	x	Customers are responsible for documenting and assigning roles and responsibilities for applicable activities. Roles and responsibilities must be understood by assigned individuals.	Customers are responsible for documenting and assigning roles and responsibilities for applicable activities. Roles and responsibilities must be understood by assigned individuals.	Customers are responsible for documenting and assigning roles and responsibilities for applicable activities. Roles and responsibilities must be understood by assigned individuals.	Customers are responsible for documenting and assigning roles and responsibilities for applicable activities. Roles and responsibilities must be understood by assigned individuals.	Google has documented and assigned roles and responsibilities for applicable activities. Roles and responsibilities are understood by assigned individuals.
10.2.1 Audit logs are enabled and active for all system components and cardholder data.	10.1	x	x	Customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their VM instances, networks and applications in alignment with PCI DSS requirements. Customers may use Cloud Audit Logs to meet logging requirements.	Customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their VM instances, networks and applications in alignment with PCI DSS requirements. Customers may use Cloud Audit Logs to meet logging requirements.	Customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their VM instances, networks and applications in alignment with PCI DSS requirements. Customers may use Cloud Audit Logs to meet logging requirements.	Customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their VM instances, networks and applications in alignment with PCI DSS requirements. Customers may use Cloud Audit Logs to meet logging requirements. Customers should enable Access Transparency logs to record and monitor the actions taken by Google personnel.	Google has PCI DSS compliance responsibility for dedicated internal Google Production and management network systems.
10.2.1.1 Audit logs capture all individual user access to cardholder data.	10.2.1		x	Customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their VM instances, networks and applications in alignment with PCI DSS requirements.	Customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their VM instances, networks and applications in alignment with PCI DSS requirements.	Customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their VM instances, networks and applications in alignment with PCI DSS requirements.	Customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their VM instances, networks and applications in alignment with PCI DSS requirements.Customers should enable Access Transparency logs to	Not Applicable.

PCI DSS 4.0 Requirements	PCI DSS 3.2.1	GCP	Customer	Compute	Networking	Storage	Security & Identity	Google Responsibility Summary
							record and monitor the actions taken by Google personnel.	
10.2.1.2 Audit logs capture all actions taken by any individual with administrative access, including any interactive use of application or system accounts.	10.2.2	x	x	Customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their VM instances, networks and applications in alignment with PCI DSS requirements.	Customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their VM instances, networks and applications in alignment with PCI DSS requirements.	Customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their VM instances, networks and applications in alignment with PCI DSS requirements.	Customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their VM instances, networks and applications in alignment with PCI DSS requirements.	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with this requirement.
10.2.1.3 Audit logs capture all access to audit logs.	10.2.3	x	x	Customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their VM instances, networks and applications in alignment with PCI DSS requirements.	Customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their VM instances, networks and applications in alignment with PCI DSS requirements.	Customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their VM instances, networks and applications in alignment with PCI DSS requirements.	Customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their VM instances, networks and applications in alignment with PCI DSS requirements.	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with this requirement.
10.2.1.4 Audit logs capture all invalid logical access attempts.	10.2.4	x	x	Customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their VM instances, networks and applications in alignment with PCI DSS requirements.	Customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their VM instances, networks and applications in alignment with PCI DSS requirements.	Customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their VM instances, networks and applications in alignment with PCI DSS requirements.	Customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their VM instances, networks and applications in alignment with PCI DSS requirements.	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with this requirement.
10.2.1.5 Audit logs capture all changes to identification and authentication credentials including, but not limited to: • Creation of new accounts. • Elevation of privileges. • All changes, additions, or deletions to accounts with administrative access.	10.2.5	x	x	Customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their VM instances, networks and applications in alignment with PCI DSS requirements.	Customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their VM instances, networks and applications in alignment with PCI DSS requirements.	Customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their VM instances, networks and applications in alignment with PCI DSS requirements.	Customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their VM instances, networks and applications in alignment with PCI DSS requirements.	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with this requirement.
10.2.1.6 Audit logs capture the following: • All initialization of new audit logs, and • All starting, stopping, or pausing of the existing audit logs.	10.2.6	x	x	Customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their VM instances, networks and applications in alignment with PCI DSS requirements.	Customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their VM instances, networks and applications in alignment with PCI DSS requirements.	Customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their VM instances, networks and applications in alignment with PCI DSS requirements.	Customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their VM instances, networks and applications in alignment with PCI DSS requirements.	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with this requirement.
10.2.1.7 Audit logs capture all creation and deletion of system-level objects.	10.2.7	x	x	Customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their VM instances, networks and applications in alignment with PCI DSS requirements.	Customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their VM instances, networks and applications in alignment with PCI DSS requirements.	Customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their VM instances, networks and applications in alignment with PCI DSS requirements.	Customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their VM instances, networks and applications in alignment with PCI DSS requirements.	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with this requirement.
10.2.2 Audit logs record the following details for each auditable event: • User identification. • Type of event. • Date and time. • Success and failure indication. • Origination of event. • Identity or name of affected data, system component, resource, or service (for example, name and protocol).	10.3 - 10.3.6	x	x	Customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their VM instances, networks and applications in alignment with PCI DSS requirements.	Customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their VM instances, networks and applications in alignment with PCI DSS requirements.	Customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their VM instances, networks and applications in alignment with PCI DSS requirements.	Customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their VM instances, networks and applications in alignment with PCI DSS requirements.	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with this requirement.

PCI DSS 4.0 Requirements	PCI DSS 3.2.1	GCP	Customer	Compute	Networking	Storage	Security & Identity	Google Responsibility Summary
10.3.1 Read access to audit logs files is limited to those with a job-related need.	10.5.1	x	x	Customers are responsible for setting permissions and access controls for audit logs. Identity Access Management (IAM) can be used to set permissions for accounts with access to online and offline log storage locations. Customers are responsible to log and monitor their VM instances in alignment with PCI DSS requirements.	Customers are responsible for setting permissions and access controls for audit logs. Identity Access Management (IAM) can be used to set permissions for accounts with access to online and offline log storage locations. Customers are responsible to log and monitor their VM instances in alignment with PCI DSS requirements.	Customers are responsible for setting permissions and access controls for audit logs. Identity Access Management (IAM) can be used to set permissions for accounts with access to online and offline log storage locations. Customers are responsible to log and monitor their VM instances in alignment with PCI DSS requirements.	Customers are responsible for setting permissions and access controls for audit logs. Identity Access Management (IAM) can be used to set permissions for accounts with access to online and offline log storage locations. Customers are responsible to log and monitor their VM instances in alignment with PCI DSS requirements.	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with this requirement.
10.3.2 Audit log files are protected to prevent modifications by individuals.	10.5.2	x	x	Customers are responsible for setting permissions and access controls for audit logs. Identity Access Management (IAM) can be used to set permissions for accounts with access to online and offline log storage locations. Customers are responsible to log and monitor their VM instances in alignment with PCI DSS requirements.	Customers are responsible for setting permissions and access controls for audit logs. Identity Access Management (IAM) can be used to set permissions for accounts with access to online and offline log storage locations. Customers are responsible to log and monitor their VM instances in alignment with PCI DSS requirements.	Customers are responsible for setting permissions and access controls for audit logs. Identity Access Management (IAM) can be used to set permissions for accounts with access to online and offline log storage locations. Customers are responsible to log and monitor their VM instances in alignment with PCI DSS requirements.	Customers are responsible for setting permissions and access controls for audit logs. Identity Access Management (IAM) can be used to set permissions for accounts with access to online and offline log storage locations. Customers are responsible to log and monitor their VM instances in alignment with PCI DSS requirements.	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with this requirement.
10.3.3 Audit log files, including those for external- facing technologies, are promptly backed up to a secure, central, internal log server(s) or other media that is difficult to modify.	10.5.3, 10.5.4	x	x	Customers are responsible for setting permissions and access controls for audit logs. Identity Access Management (IAM) can be used to set permissions for accounts with access to online and offline log storage locations. Customers are responsible to log and monitor their VM instances in alignment with PCI DSS requirements.	Customers are responsible for setting permissions and access controls for audit logs. Identity Access Management (IAM) can be used to set permissions for accounts with access to online and offline log storage locations. Customers are responsible to log and monitor their VM instances in alignment with PCI DSS requirements.	Customers are responsible for setting permissions and access controls for audit logs. Identity Access Management (IAM) can be used to set permissions for accounts with access to online and offline log storage locations. Customers are responsible to log and monitor their VM instances in alignment with PCI DSS requirements.	Customers are responsible for setting permissions and access controls for audit logs. Identity Access Management (IAM) can be used to set permissions for accounts with access to online and offline log storage locations. Customers are responsible to log and monitor their VM instances in alignment with PCI DSS requirements.	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with this requirement.
10.3.4 File integrity monitoring or change-detection mechanisms is used on audit logs to ensure that existing log data cannot be changed without generating alerts.	10.5.5	x	x	Customers are responsible for setting permissions and access controls for audit logs. Identity Access Management (IAM) can be used to set permissions for accounts with access to online and offline log storage locations. Customers are responsible to log and monitor their VM instances in alignment with PCI DSS requirements.	Customers are responsible for setting permissions and access controls for audit logs. Identity Access Management (IAM) can be used to set permissions for accounts with access to online and offline log storage locations. Customers are responsible to log and monitor their VM instances in alignment with PCI DSS requirements.	Customers are responsible for setting permissions and access controls for audit logs. Identity Access Management (IAM) can be used to set permissions for accounts with access to online and offline log storage locations. Customers are responsible to log and monitor their VM instances in alignment with PCI DSS requirements.	Customers are responsible for setting permissions and access controls for audit logs. Identity Access Management (IAM) can be used to set permissions for accounts with access to online and offline log storage locations. Customers are responsible to log and monitor their VM instances in alignment with PCI DSS requirements.	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with this requirement.
10.4.1 The following audit logs are reviewed at least once daily: • All security events. • Logs of all system components that store, process, or transmit CHD and/or SAD. • Logs of all critical system components. • Logs of all servers and system components that perform security functions (for example, network security controls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers).	10.6.1	x	x	Customers are responsible for review (automated or manual) of audit logs, and for logging and monitoring their VPC networks, storage buckets and VM instances in alignment with PCI DSS requirements.	Customers are responsible for review (automated or manual) of audit logs, and for logging and monitoring their VPC networks, storage buckets and VM instances in alignment with PCI DSS requirements.	Customers are responsible for review (automated or manual) of audit logs, and for logging and monitoring their VPC networks, storage buckets and VM instances in alignment with PCI DSS requirements.	Customers are responsible for review (automated or manual) of audit logs, and for logging and monitoring their VPC networks, storage buckets and VM instances in alignment with PCI DSS requirements.	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with this requirement.

PCI DSS 4.0 Requirements	PCI DSS 3.2.1	GCP	Customer	Compute	Networking	Storage	Security & Identity	Google Responsibility Summary
10.4.1.1 Automated mechanisms are used to perform audit log reviews.	*New*	x	x	Customers are responsible for review (automated or manual) of audit logs, and for logging and monitoring their VPC networks, storage buckets and VM instances in alignment with PCI DSS requirements.	Customers are responsible for review (automated or manual) of audit logs, and for logging and monitoring their VPC networks, storage buckets and VM instances in alignment with PCI DSS requirements.	Customers are responsible for review (automated or manual) of audit logs, and for logging and monitoring their VPC networks, storage buckets and VM instances in alignment with PCI DSS requirements.	Customers are responsible for review (automated or manual) of audit logs, and for logging and monitoring their VPC networks, storage buckets and VM instances in alignment with PCI DSS requirements.	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with this requirement.
10.4.2 Logs of all other system components (those not specified in Requirement 10.4.1) are reviewed periodically.	10.6.2	x	x	Customers are responsible for review (automated or manual) of audit logs, and for logging and monitoring their VPC networks, storage buckets and VM instances in alignment with PCI DSS requirements.	Customers are responsible for review (automated or manual) of audit logs, and for logging and monitoring their VPC networks, storage buckets and VM instances in alignment with PCI DSS requirements.	Customers are responsible for review (automated or manual) of audit logs, and for logging and monitoring their VPC networks, storage buckets and VM instances in alignment with PCI DSS requirements.	Customers are responsible for review (automated or manual) of audit logs, and for logging and monitoring their VPC networks, storage buckets and VM instances in alignment with PCI DSS requirements.	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with this requirement.
10.4.2.1 The frequency of periodic log reviews for all other system components (not defined in Requirement 10.4.1) is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1	*New*		x	Customers are responsible for conducting a targeted risk analysis of their control environment and determining control frequency to meet applicable PCI DSS requirements.	Customers are responsible for conducting a targeted risk analysis of their control environment and determining control frequency to meet applicable PCI DSS requirements.	Customers are responsible for conducting a targeted risk analysis of their control environment and determining control frequency to meet applicable PCI DSS requirements.	Customers are responsible for conducting a targeted risk analysis of their control environment and determining control frequency to meet applicable PCI DSS requirements.	Not Applicable.
10.4.3 Exceptions and anomalies identified during the review process are addressed.	10.6.3	x	x	Customers are responsible for review (automated or manual) of audit logs, and for logging and monitoring their VPC networks, storage buckets and VM instances in alignment with PCI DSS requirements.	Customers are responsible for review (automated or manual) of audit logs, and for logging and monitoring their VPC networks, storage buckets and VM instances in alignment with PCI DSS requirements.	Customers are responsible for review (automated or manual) of audit logs, and for logging and monitoring their VPC networks, storage buckets and VM instances in alignment with PCI DSS requirements.	Customers are responsible for review (automated or manual) of audit logs, and for logging and monitoring their VPC networks, storage buckets and VM instances in alignment with PCI DSS requirements.	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with this requirement.
10.5.1 Retain audit log history for at least 12 months, with at least the most recent three months immediately available for analysis.	10.7	x	x	Customers are responsible for review (automated or manual) of audit logs, and for logging and monitoring their VPC networks, storage buckets and VM instances in alignment with PCI DSS requirements.	Customers are responsible for review (automated or manual) of audit logs, and for logging and monitoring their VPC networks, storage buckets and VM instances in alignment with PCI DSS requirements.	Customers are responsible for review (automated or manual) of audit logs, and for logging and monitoring their VPC networks, storage buckets and VM instances in alignment with PCI DSS requirements.	Customers are responsible for review (automated or manual) of audit logs, and for logging and monitoring their VPC networks, storage buckets and VM instances in alignment with PCI DSS requirements.	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with this requirement.
10.6.1 System clocks and time are synchronized using time-synchronization technology.	10.4	x	x	Customers are responsible for appropriately managing network time protocol (NTP) configuration for their system components.	Customers are responsible for appropriately managing network time protocol (NTP) configuration for their system components.	Customers are responsible for appropriately managing network time protocol (NTP) configuration for their system components.	Customers are responsible for appropriately managing network time protocol (NTP) configuration for their system components.	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with this requirement.
10.6.2 Systems are configured to the correct and consistent time as follows: • One or more designated time servers are in use. • Only the designated central time server(s) receives time from external sources. • Time received from external sources is based on International Atomic Time or Coordinated Universal Time (UTC). • The designated time server(s) accept time updates only from specific industry-accepted external sources. • Where there is more than one designated time server, the time servers peer with one another to keep accurate time. • Internal systems receive time information only from designated central time server(s).	10.4.1, 10.4.3	x	x	Customers are responsible for appropriately managing network time protocol (NTP) configuration for their system components.	Customers are responsible for appropriately managing network time protocol (NTP) configuration for their system components.	Customers are responsible for appropriately managing network time protocol (NTP) configuration for their system components.	Customers are responsible for appropriately managing network time protocol (NTP) configuration for their system components.	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with this requirement.

PCI DSS 4.0 Requirements	PCI DSS 3.2.1	GCP	Customer	Compute	Networking	Storage	Security & Identity	Google Responsibility Summary
10.6.3 Time synchronization settings and data are protected as follows: • Access to time data is restricted to only personnel with a business need. • Any changes to time settings on critical systems are logged, monitored, and reviewed.	10.4.2	x	x	Customers are responsible for appropriately managing network time protocol (NTP) configuration for their VM instances.	Customers are responsible for appropriately managing network time protocol (NTP) configuration for their VM instances.	Customers are responsible for appropriately managing network time protocol (NTP) configuration for their VM instances.	Customers are responsible for appropriately managing network time protocol (NTP) configuration for their VM instances.	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with this requirement.
10.7.1 Additional requirement for service providers only: Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: • Network security controls. • IDS/IPS. • FIM. • Anti-malware solutions. • Physical access controls. • Logical access controls. • Audit logging mechanisms. • Segmentation controls (if used).	10.8	x	x	Customers are responsible for ensuring a process is implemented for timely detection and reporting of failures of critical security control systems; failures are addressed promptly.	Customers are responsible for ensuring a process is implemented for timely detection and reporting of failures of critical security control systems; failures are addressed promptly.	Customers are responsible for ensuring a process is implemented for timely detection and reporting of failures of critical security control systems; failures are addressed promptly.	Customers are responsible for ensuring a process is implemented for timely detection and reporting of failures of critical security control systems; failures are addressed promptly. Customers may use services such as Cloud IDS, Security Command Center, Cloud Monitoring, and Cloud Networking services to help achieve some of these security measures.	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with this requirement; failures of critical security control systems are addressed promptly.
10.7.2 Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: • Network security controls. • IDS/IPS. • Change-detection mechanisms. • Anti-malware solutions. • Physical access controls. • Logical access controls. • Audit logging mechanisms. • Segmentation controls (if used). • Audit log review mechanisms. • Automated security testing tools (if used).	*New*	x	x	Customers are responsible for ensuring a process is implemented for timely detection and reporting of failures of critical security control systems; failures are addressed promptly.	Customers are responsible for ensuring a process is implemented for timely detection and reporting of failures of critical security control systems; failures are addressed promptly.	Customers are responsible for ensuring a process is implemented for timely detection and reporting of failures of critical security control systems; failures are addressed promptly.	Customers are responsible for ensuring a process is implemented for timely detection and reporting of failures of critical security control systems; failures are addressed promptly.	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with this requirement; failures of critical security control systems are addressed promptly.
10.7.3 Failures of any critical security controls systems are responded to promptly, including but not limited to: • Restoring security functions. • Identifying and documenting the duration (date and time from start to end) of the security failure. • Identifying and documenting the cause(s) of failure and documenting required remediation. • Identifying and addressing any security issues that arose during the failure. • Determining whether further actions are required as a result of the security failure. • Implementing controls to prevent the cause of failure from reoccurring. • Resuming monitoring of security controls.	10.8.1	x	x	Customers are responsible for ensuring a process is implemented for timely detection and reporting of failures of critical security control systems; failures are addressed promptly.	Customers are responsible for ensuring a process is implemented for timely detection and reporting of failures of critical security control systems; failures are addressed promptly.	Customers are responsible for ensuring a process is implemented for timely detection and reporting of failures of critical security control systems; failures are addressed promptly.	Customers are responsible for ensuring a process is implemented for timely detection and reporting of failures of critical security control systems; failures are addressed promptly.	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with this requirement; failures of critical security control systems are addressed promptly.
Requirement 11: Test Security of Systems and Networks Regularly								

PCI DSS 4.0 Requirements	PCI DSS 3.2.1	GCP	Customer	Compute	Networking	Storage	Security & Identity	Google Responsibility Summary
11.1.1 All security policies and operational procedures that are identified in Requirement 11 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	11.6		x	Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Not Applicable
11.1.2 Roles and responsibilities for performing activities in Requirement 11 are documented, assigned, and understood.	*New*	x	x	Customers are responsible for documenting and assigning roles and responsibilities for applicable activities. Roles and responsibilities must be understood by assigned individuals.	Customers are responsible for documenting and assigning roles and responsibilities for applicable activities. Roles and responsibilities must be understood by assigned individuals.	Customers are responsible for documenting and assigning roles and responsibilities for applicable activities. Roles and responsibilities must be understood by assigned individuals.	Customers are responsible for documenting and assigning roles and responsibilities for applicable activities. Roles and responsibilities must be understood by assigned individuals.	Google has documented and assigned roles and responsibilities for applicable activities. Roles and responsibilities are understood by assigned individuals.
11.2.1 Authorized and unauthorized wireless access points are managed as follows: • The presence of wireless (Wi-Fi) access points is tested for, • All authorized and unauthorized wireless access points are detected and identified, • Testing, detection, and identification occurs at least once every three months. • If automated monitoring is used, personnel are notified via generated alerts.	11.1	x		Not Applicable	Not Applicable	Not Applicable	Not Applicable	Google is responsible for checking for the presence of wireless access points and similar technologies within its own physical environment and in scope networks.
11.2.2 An inventory of authorized wireless access points is maintained, including a documented business justification.	11.1.1	x		Not Applicable	Not Applicable	Not Applicable	Not Applicable	Google is responsible for checking for the presence of wireless access points and similar technologies within its own physical environment and in scope networks.
11.3.1 Internal vulnerability scans are performed as follows: • At least once every three months. • High-risk and critical vulnerabilities (per the entity's vulnerability risk rankings defined at Requirement 6.3.1) are resolved. • Rescans are performed that confirm all high- risk and critical vulnerabilities (as noted above) have been resolved. • Scan tool is kept up to date with latest vulnerability information. • Scans are performed by qualified personnel and organizational independence of the tester exists.	11.2.1	x	x	Customers are responsible for internal vulnerability scanning of all system components within their cardholder data environment, including all applicable GCP Products (GCE, GCS, VPC, etc.).	Customers are responsible for internal vulnerability scanning of all system components within their cardholder data environment, including all applicable GCP Products (GCE, GCS, VPC, etc.).	Customers are responsible for internal vulnerability scanning of all system components within their cardholder data environment, including all applicable GCP Products (GCE, GCS, VPC, etc.).	Customers are responsible for internal vulnerability scanning of all system components within their cardholder data environment, including all applicable GCP Products (GCE, GCS, VPC, etc.).	Google is responsible for conducting quarterly internal vulnerability scans on systems and the infrastructure underlying GCP. Google is also responsible for scanning of Google managed API endpoints and Cloud Load Balancer IP addresses.
11.3.1.1 All other applicable vulnerabilities (those not ranked as high-risk or critical per the entity's vulnerability risk rankings defined at Requirement 6.3.1) are managed as follows: • Addressed based on the risk defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1. • Rescans are conducted as needed.	*New*		x	Customers are responsible for conducting a targeted risk analysis of their control environment and determining control frequency to meet applicable PCI DSS requirements.	Customers are responsible for conducting a targeted risk analysis of their control environment and determining control frequency to meet applicable PCI DSS requirements.	Customers are responsible for conducting a targeted risk analysis of their control environment and determining control frequency to meet applicable PCI DSS requirements.	Customers are responsible for conducting a targeted risk analysis of their control environment and determining control frequency to meet applicable PCI DSS requirements.	Not Applicable

PCI DSS 4.0 Requirements	PCI DSS 3.2.1	GCP	Customer	Compute	Networking	Storage	Security & Identity	Google Responsibility Summary
11.3.1.2 Internal vulnerability scans are performed via authenticated scanning as follows: • Systems that are unable to accept credentials for authenticated scanning are documented. • Sufficient privileges are used for those systems that accept credentials for scanning. • If accounts used for authenticated scanning can be used for interactive login, they are managed in accordance with Requirement 8.2.2.	*New*	x	x	Customers are responsible for internal vulnerability scanning of all system components within their cardholder data environment, including all applicable GCP Products (GCE, GCS, VPC, etc.).	Customers are responsible for internal vulnerability scanning of all system components within their cardholder data environment, including all applicable GCP Products (GCE, GCS, VPC, etc.).	Customers are responsible for internal vulnerability scanning of all system components within their cardholder data environment, including all applicable GCP Products (GCE, GCS, VPC, etc.).	Customers are responsible for internal vulnerability scanning of all system components within their cardholder data environment, including all applicable GCP Products (GCE, GCS, VPC, etc.).	Google is responsible for conducting quarterly internal vulnerability scans on systems and the infrastructure underlying GCP. Google is also responsible for scanning of Google managed API endpoints and Cloud Load Balancer IP addresses.
11.3.1.3 Internal vulnerability scans are performed after any significant change as follows: • High-risk and critical vulnerabilities (per the entity's vulnerability risk rankings defined at Requirement 6.3.1) are resolved. • Rescans are conducted as needed. • Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV).	11.2.3	x	x	Customers are responsible for internal vulnerability scanning of all system components within their cardholder data environment, including all applicable GCP Products (GCE, GCS, VPC, etc.).	Customers are responsible for internal vulnerability scanning of all system components within their cardholder data environment, including all applicable GCP Products (GCE, GCS, VPC, etc.).	Customers are responsible for internal vulnerability scanning of all system components within their cardholder data environment, including all applicable GCP Products (GCE, GCS, VPC, etc.).	Customers are responsible for internal vulnerability scanning of all system components within their cardholder data environment, including all applicable GCP Products (GCE, GCS, VPC, etc.).	Google is responsible for conducting quarterly internal vulnerability scans on systems and the infrastructure underlying GCP. Google is also responsible for scanning of Google managed API endpoints and Cloud Load Balancer IP addresses.
11.3.2 External vulnerability scans are performed as follows: • At least once every three months. • By a PCI SSC Approved Scanning Vendor (ASV). • Vulnerabilities are resolved and ASV Program Guide requirements for a passing scan are met. • Rescans are performed as needed to confirm that vulnerabilities are resolved per the ASV Program Guide requirements for a passing scan.	11.2.2	x	x	Customers are responsible for external vulnerability scanning of all applicable system components within their cardholder data environment, in accordance with PCI DSS requirements. (Note: External vulnerability scans should only include the customer-managed endpoints, and not GCP-managed endpoints as they are tested as part of GCP PCI DSS compliance).	Customers are responsible for external vulnerability scanning of all applicable system components within their cardholder data environment, in accordance with PCI DSS requirements. (Note: External vulnerability scans should only include the customer-managed endpoints, and not GCP-managed endpoints as they are tested as part of GCP PCI DSS compliance).	Customers are responsible for external vulnerability scanning of all applicable system components within their cardholder data environment, in accordance with PCI DSS requirements. (Note: External vulnerability scans should only include the customer-managed endpoints, and not GCP-managed endpoints as they are tested as part of GCP PCI DSS compliance).	Customers are responsible for external vulnerability scanning of all applicable system components within their cardholder data environment, in accordance with PCI DSS requirements. (Note: External vulnerability scans should only include the customer-managed endpoints, and not GCP-managed endpoints as they are tested as part of GCP PCI DSS compliance).	Google is responsible for conducting quarterly external vulnerability scans on systems and the infrastructure underlying GCP. Google is also responsible for scanning of Google managed API endpoints and Cloud Load Balancer IP addresses.
11.3.2.1 External vulnerability scans are performed after any significant change as follows: • Vulnerabilities that are scored 4.0 or higher by the CVSS are resolved. • Rescans are conducted as needed. • Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV).	11.2.3	x	x	Customers are responsible for external vulnerability scanning of all applicable system components within their cardholder data environment, in accordance with PCI DSS requirements. (Note: External vulnerability scans should only include the customer-managed endpoints, and not GCP-managed endpoints as they are tested as part of GCP PCI DSS compliance).	Customers are responsible for external vulnerability scanning of all applicable system components within their cardholder data environment, in accordance with PCI DSS requirements. (Note: External vulnerability scans should only include the customer-managed endpoints, and not GCP-managed endpoints as they are tested as part of GCP PCI DSS compliance).	Customers are responsible for external vulnerability scanning of all applicable system components within their cardholder data environment, in accordance with PCI DSS requirements. (Note: External vulnerability scans should only include the customer-managed endpoints, and not GCP-managed endpoints as they are tested as part of GCP PCI DSS compliance).	Customers are responsible for external vulnerability scanning of all applicable system components within their cardholder data environment, in accordance with PCI DSS requirements. (Note: External vulnerability scans should only include the customer-managed endpoints, and not GCP-managed endpoints as they are tested as part of GCP PCI DSS compliance).	Google is responsible for conducting quarterly external vulnerability scans on systems and the infrastructure underlying GCP. Google is also responsible for scanning of Google managed API endpoints and Cloud Load Balancer IP addresses.

PCI DSS 4.0 Requirements	PCI DSS 3.2.1	GCP	Customer	Compute	Networking	Storage	Security & Identity	Google Responsibility Summary
11.4.1 A penetration testing methodology is defined, documented, and implemented by the entity, and includes: • Industry-accepted penetration testing approaches. • Coverage for the entire CDE perimeter and critical systems. • Testing from both inside and outside the network. • Testing to validate any segmentation and scope-reduction controls. • Application-layer penetration testing to identify, at a minimum, the vulnerabilities listed in Requirement 6.2.4. • Network-layer penetration tests that encompass all components that support network functions as well as operating systems. • Review and consideration of threats and vulnerabilities experienced in the last 12 months. • Documented approach to assessing and addressing the risk posed by exploitable vulnerabilities and security weaknesses found during penetration testing. • Retention of penetration testing results and remediation activities results for at least 12 months.	11.3	x	x	Customers are responsible for defining, documenting, and implementing a penetration testing methodology, in accordance with PCI DSS requirements.	Customers are responsible for defining, documenting, and implementing a penetration testing methodology, in accordance with PCI DSS requirements.	Customers are responsible for defining, documenting, and implementing a penetration testing methodology, in accordance with PCI DSS requirements.	Customers are responsible for defining, documenting, and implementing a penetration testing methodology, in accordance with PCI DSS requirements.	Google is responsible for defining, documenting, and implementing a penetration testing methodology, in accordance with PCI DSS requirements.
11.4.2 Internal penetration testing is performed: • Per the entity's defined methodology, • At least once every 12 months • After any significant infrastructure or application upgrade or change • By a qualified internal resource or qualified external third-party • Organizational independence of the tester exists (not required to be a QSA or ASV).	11.3.2	x	x	Customers are responsible for all internal penetration testing of in-scope system components, comprising their cardholder data environment.	Customers are responsible for all internal penetration testing of in-scope system components, comprising their cardholder data environment.	Customers are responsible for all internal penetration testing of in-scope system components, comprising their cardholder data environment.	Customers are responsible for all internal penetration testing of in-scope system components, comprising their cardholder data environment. Customers may hire Mandiant to conduct external and internal penetration tests.	Google is responsible for conducting internal penetration testing on systems and infrastructure underlying GCP.
11.4.3 External penetration testing is performed: • Per the entity's defined methodology • At least once every 12 months • After any significant infrastructure or application upgrade or change • By a qualified internal resource or qualified external third party • Organizational independence of the tester exists (not required to be a QSA or ASV). (continued on next page)	11.3.1	x	x	Customers are responsible for all external penetration testing of in-scope system components, comprising their cardholder data environment. (Note: External vulnerability scans should only include the customer-managed endpoints, and not GCP-managed endpoints as they are tested as part of GCP PCI DSS compliance).	Customers are responsible for all external penetration testing of in-scope system components, comprising their cardholder data environment. (Note: External vulnerability scans should only include the customer-managed endpoints, and not GCP-managed endpoints as they are tested as part of GCP PCI DSS compliance).	Customers are responsible for all external penetration testing of in-scope system components, comprising their cardholder data environment. (Note: External vulnerability scans should only include the customer-managed endpoints, and not GCP-managed endpoints as they are tested as part of GCP PCI DSS compliance).	Customers are responsible for all external penetration testing of in-scope system components, comprising their cardholder data environment. Customers may hire Mandiant to conduct external and internal penetration tests. (Note: External vulnerability scans should only include the customer-managed endpoints, and not GCP-managed endpoints as they are tested as part of GCP PCI DSS compliance).	Google is responsible for conducting external penetration testing on systems and infrastructure underlying GCP. Google is also responsible for scanning of Google managed API endpoints and Cloud Load Balancer IP addresses.

PCI DSS 4.0 Requirements	PCI DSS 3.2.1	GCP	Customer	Compute	Networking	Storage	Security & Identity	Google Responsibility Summary
11.4.4 Exploitable vulnerabilities and security weaknesses found during penetration testing are corrected as follows: • In accordance with the entity's assessment of the risk posed by the security issue as defined in Requirement 6.3.1. • Penetration testing is repeated to verify the corrections.	11.3.3	x	x	Customers are responsible for correcting security vulnerabilities identified through their internal and external penetration testing of in-scope system components. (Note: External vulnerability scans should only include the customer-managed endpoints, and not GCP-managed endpoints as they are tested as part of GCP PCI DSS compliance).	Customers are responsible for correcting security vulnerabilities identified through their internal and external penetration testing of in-scope system components. (Note: External vulnerability scans should only include the customer-managed endpoints, and not GCP-managed endpoints as they are tested as part of GCP PCI DSS compliance).	Customers are responsible for correcting security vulnerabilities identified through their internal and external penetration testing of in-scope system components. (Note: External vulnerability scans should only include the customer-managed endpoints, and not GCP-managed endpoints as they are tested as part of GCP PCI DSS compliance).	Customers are responsible for correcting security vulnerabilities identified through their internal and external penetration testing of in-scope system components. Customers may hire Mandiant to conduct external and internal penetration tests. (Note: External vulnerability scans should only include the customer-managed endpoints, and not GCP-managed endpoints as they are tested as part of GCP PCI DSS compliance).	Google is responsible for correcting security vulnerabilities identified through internal and external penetration testing of systems and infrastructure underlying GCP.
11.4.5 If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: • At least once every 12 months and after any changes to segmentation controls/methods • Covering all segmentation controls/methods in use. • According to the entity's defined penetration testing methodology. • Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems. • Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3). • Performed by a qualified internal resource or qualified external third party. • Organizational independence of the tester exists (not required to be a QSA or ASV).	11.3.4	x	x	Customers are responsible for performing penetration testing on segmentation controls in accordance with PCI DSS requirements, and after any changes to its segmentation methods for their VM instances, storage buckets and VPC networks.	Customers are responsible for performing penetration testing on segmentation controls in accordance with PCI DSS requirements, and after any changes to its segmentation methods for their VM instances, storage buckets and VPC networks.	Customers are responsible for performing penetration testing on segmentation controls in accordance with PCI DSS requirements, and after any changes to its segmentation methods for their VM instances, storage buckets and VPC networks.	Customers are responsible for performing penetration testing on segmentation controls in accordance with PCI DSS requirements, and after any changes to its segmentation methods for their VM instances, storage buckets and VPC networks.	Google is responsible for conducting segmentation penetration testing on systems and infrastructure underlying GCP.
11.4.6 Additional requirement for service providers only: If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: • At least once every six months and after any changes to segmentation controls/methods. • Covering all segmentation controls/methods in use. • According to the entity's defined penetration testing methodology. • Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems. • Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3). • Performed by a qualified internal resource or qualified external third party.	11.3.4.1	x	x	Customers are responsible for performing penetration testing on segmentation controls in accordance with PCI DSS requirements, and after any changes to its segmentation methods for their VM instances, storage buckets and VPC networks.	Customers are responsible for performing penetration testing on segmentation controls in accordance with PCI DSS requirements, and after any changes to its segmentation methods for their VM instances, storage buckets and VPC networks.	Customers are responsible for performing penetration testing on segmentation controls in accordance with PCI DSS requirements, and after any changes to its segmentation methods for their VM instances, storage buckets and VPC networks.	Customers are responsible for performing penetration testing on segmentation controls in accordance with PCI DSS requirements, and after any changes to its segmentation methods for their VM instances, storage buckets and VPC networks.	Google is responsible for conducting segmentation penetration testing on systems and infrastructure underlying GCP.

PCI DSS 4.0 Requirements	PCI DSS 3.2.1	GCP	Customer	Compute	Networking	Storage	Security & Identity	Google Responsibility Summary
• Organizational independence of the tester exists (not required to be a QSA or ASV).								
11.4.7 Additional requirement for multi-tenant service providers only: Multi-tenant service providers support their customers for external penetration testing per Requirement 11.4.3 and 11.4.4.	*New*	x	x	Multi-tenant customers support their customers in meeting external penetration testing requirements.	Multi-tenant customers support their customers in meeting external penetration testing requirements.	Multi-tenant customers support their customers in meeting external penetration testing requirements.	Multi-tenant customers support their customers in meeting external penetration testing requirements.	Google provides customers with guidance on how to conduct penetration testing on GCP projects.
11.5.1 Intrusion-detection and/or intrusion- prevention techniques are used to detect and/or prevent intrusions into the network as follows: • All traffic is monitored at the perimeter of the CDE. • All traffic is monitored at critical points in the CDE. • Personnel are alerted to suspected compromises. • All intrusion-detection and prevention engines, baselines, and signatures are kept up to date.	11.4	x	x	Customers are responsible for implementing intrusion-detection and/or intrusion-prevention techniques, typically using Host-based IDS (HIDS), for network segments they implement and manage.	Customers are responsible for implementing intrusion-detection and/or intrusion-prevention techniques, typically using Host-based IDS (HIDS), for network segments they implement and manage.	Customers are responsible for implementing intrusion-detection and/or intrusion-prevention techniques, typically using Host-based IDS (HIDS), for network segments they implement and manage.	Customers are responsible for implementing intrusion-detection and/or intrusion-prevention techniques, typically using Host-based IDS (HIDS), for network segments they implement and manage. Customers may use Cloud IDS to detect intrusions into the network.	Google is responsible for intrusion detection of Google Cloud systems and infrastructure underlying GCP in compliance with this requirement.
11.5.1.1 Additional requirement for service providers only: Intrusion-detection and/or intrusion-prevention techniques detect, alert on/prevent, and address covert malware communication channels.	*New*	x	x	Customers are responsible for implementing intrusion-detection and/or intrusion- prevention techniques, typically using Host-based IDS (HIDS), for network segments they implement and manage.	Customers are responsible for implementing intrusion-detection and/or intrusion- prevention techniques, typically using Host-based IDS (HIDS), for network segments they implement and manage.	Customers are responsible for implementing intrusion-detection and/or intrusion- prevention techniques, typically using Host-based IDS (HIDS), for network segments they implement and manage.	Customers are responsible for implementing intrusion-detection and/or intrusion- prevention techniques, typically using Host-based IDS (HIDS), for network segments they implement and manage.	Google is responsible for intrusion detection of Google Cloud systems and infrastructure underlying GCP in compliance with this requirement.
11.5.2 A change-detection mechanism (for example, file integrity monitoring tools) is deployed as follows: • To alert personnel to unauthorized modification (including changes, additions, and deletions) of critical files. • To perform critical file comparisons at least once weekly.	11.5	x	x	Customers are responsible for managing change-detection mechanisms for their VM instances, storage buckets and VPC networks.	Customers are responsible for managing change-detection mechanisms for their VM instances, storage buckets and VPC networks.	Customers are responsible for managing change-detection mechanisms for their VM instances, storage buckets and VPC networks.	Customers are responsible for managing change-detection mechanisms for their VM instances, storage buckets and VPC networks. Customers may procure change-detection tools such as file integrity monitoring tools from the Google Cloud Marketplace.	Google is responsible for change-detection mechanisms on the systems and infrastructure underlying GCP in compliance with this requirement.
11.6.1 A change- and tamper-detection mechanism is deployed as follows: • To alert personnel to unauthorized modification (including indicators of compromise, changes, additions, and deletions) to the HTTP headers and the contents of payment pages as received by the consumer browser. • The mechanism is configured to evaluate the received HTTP header and payment page. • The mechanism functions are performed as follows: – At least once every seven days OR – Periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1).	*New*		x	Customers are responsible for managing change-detection mechanisms for their VM instances, storage buckets and VPC networks.	Customers are responsible for managing change-detection mechanisms for their VM instances, storage buckets and VPC networks.	Customers are responsible for managing change-detection mechanisms for their VM instances, storage buckets and VPC networks.	Customers are responsible for managing change-detection mechanisms for their VM instances, storage buckets and VPC networks. Customers may procure change-detection tools such as file integrity monitoring tools from the Google Cloud Marketplace.	Not Applicable.
Requirement 12: Support Information Security with Organizational Policies and Programs								

PCI DSS 4.0 Requirements	PCI DSS 3.2.1	GCP	Customer	Compute	Networking	Storage	Security & Identity	Google Responsibility Summary
12.1.1 An overall information security policy is: • Established. • Published. • Maintained. • Disseminated to all relevant personnel, as well as to relevant vendors and business partners.	12.1		x	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Not Applicable
12.1.2 The information security policy is: • Reviewed at least once every 12 months. • Updated as needed to reflect changes to business objectives or risks to the environment.	12.1.1		x	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Not Applicable
12.1.3 The security policy clearly defines information security roles and responsibilities for all personnel, and all personnel are aware of and acknowledge their information security responsibilities.	12.4		x	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Not Applicable
12.1.4 Responsibility for information security is formally assigned to a Chief Information Security Officer or other information security knowledgeable member of executive management.	12.5, 12.5.1 – 12.5.5		x	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Not Applicable
12.2.1 Acceptable use policies for end-user technologies are documented and implemented, including: • Explicit approval by authorized parties. • Acceptable uses of the technology. • List of products approved by the company for employee use, including hardware and software.	12.3, 12.3.1 – 12.3.9		x	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Not Applicable
12.3.1 Each PCI DSS requirement that provides flexibility for how frequently it is performed (for example, requirements to be performed periodically) is supported by a targeted risk analysis that is documented and includes: • Identification of the assets being protected. • Identification of the threat(s) that the requirement is protecting against. • Identification of factors that contribute to the likelihood and/or impact of a threat being realized. • Resulting analysis that determines, and includes justification for, how frequently the requirement must be performed to minimize the likelihood of the threat being realized. • Review of each targeted risk analysis at least once every 12 months to determine whether the results are still valid or if an updated risk analysis is needed. • Performance of updated risk analyses when needed, as determined by the annual review.	*New*		x	Customers are responsible for conducting a targeted risk analysis of their control environment and determining control frequency to meet applicable PCI DSS requirements.	Customers are responsible for conducting a targeted risk analysis of their control environment and determining control frequency to meet applicable PCI DSS requirements.	Customers are responsible for conducting a targeted risk analysis of their control environment and determining control frequency to meet applicable PCI DSS requirements.	Customers are responsible for conducting a targeted risk analysis of their control environment and determining control frequency to meet applicable PCI DSS requirements.	Not Applicable

PCI DSS 4.0 Requirements	PCI DSS 3.2.1	GCP	Customer	Compute	Networking	Storage	Security & Identity	Google Responsibility Summary
12.3.2 A targeted risk analysis is performed for each PCI DSS requirement that the entity meets with the customized approach, to include: • Documented evidence detailing each element specified in Appendix D: Customized Approach (including, at a minimum, a controls matrix and risk analysis). • Approval of documented evidence by senior management. • Performance of the targeted analysis of risk at least once every 12 months.	*New*		x	Customers are responsible for conducting a targeted risk analysis of their control environment and determining control frequency to meet applicable PCI DSS requirements.	Customers are responsible for conducting a targeted risk analysis of their control environment and determining control frequency to meet applicable PCI DSS requirements.	Customers are responsible for conducting a targeted risk analysis of their control environment and determining control frequency to meet applicable PCI DSS requirements.	Customers are responsible for conducting a targeted risk analysis of their control environment and determining control frequency to meet applicable PCI DSS requirements.	Not Applicable
12.3.3 Cryptographic cipher suites and protocols in use are documented and reviewed at least once every 12 months, including at least the following: • An up-to-date inventory of all cryptographic cipher suites and protocols in use, including purpose and where used. • Active monitoring of industry trends regarding continued viability of all cryptographic cipher suites and protocols in use. • A documented strategy to respond to anticipated changes in cryptographic vulnerabilities.	*New*		x	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Not Applicable
12.3.4 Hardware and software technologies in use are reviewed at least once every 12 months, including at least the following: • Analysis that the technologies continue to receive security fixes from vendors promptly. • Analysis that the technologies continue to support (and do not preclude) the entity's PCI DSS compliance. • Documentation of any industry announcements or trends related to a technology, such as when a vendor has announced "end of life" plans for a technology. • Documentation of a plan, approved by senior management, to remediate outdated technologies, including those for which vendors have announced "end of life" plans.	*New*		x	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Not Applicable
12.4.1 Additional requirement for service providers only: Responsibility is established by executive management for the protection of cardholder data and a PCI DSS compliance program to include: • Overall accountability for maintaining PCI DSS compliance. • Defining a charter for a PCI DSS compliance program and communication to executive management.	12.11, 12.11.1		x	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Not Applicable
12.4.2 Additional requirement for service providers only: Reviews are performed at least once every three months to confirm that personnel are performing their tasks in accordance with all security policies and operational procedures. Reviews are performed by personnel other than those responsible for performing the given task and include, but are not limited to, the following tasks: • Daily log reviews. • Configuration reviews for network security controls.	12.11, 12.11.1		x	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Not Applicable

PCI DSS 4.0 Requirements	PCI DSS 3.2.1	GCP	Customer	Compute	Networking	Storage	Security & Identity	Google Responsibility Summary
• Applying configuration standards to new systems. • Responding to security alerts. • Change-management processes.								
12.4.2.1 Additional requirement for service providers only: Reviews conducted in accordance with Requirement 12.4.2 are documented to include: • Results of the reviews. • Documented remediation actions taken for any tasks that were found to not be performed at Requirement 12.4.2. • Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program.	12.11, 12.11.1		x	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Not Applicable
12.5.1 An inventory of system components that are in scope for PCI DSS, including a description of function/use, is maintained and kept current.	2.4		x	Customers are responsible for maintaining an inventory of system components that are in scope for their cardholder data environment/ PCI DSS.	Customers are responsible for maintaining an inventory of system components that are in scope for their cardholder data environment/ PCI DSS.	Customers are responsible for maintaining an inventory of system components that are in scope for their cardholder data environment/ PCI DSS.	Customers are responsible for maintaining an inventory of system components that are in scope for their cardholder data environment/ PCI DSS. Customers may use Cloud Asset Inventory to view assets deployed in GCP.	Not Applicable
12.5.2 PCI DSS scope is documented and confirmed by the entity at least once every 12 months and upon significant change to the in-scope environment. At a minimum, the scoping validation includes: • Identifying all data flows for the various payment stages (for example, authorization, capture settlement, chargebacks, and refunds) and acceptance channels (for example, card-present, card-not-present, and e-commerce). • Updating all data-flow diagrams per Requirement 1.2.4. • Identifying all locations where account data is stored, processed, and transmitted, including but not limited to: 1) any locations outside of the currently defined CDE, 2) applications that process CHD, 3) transmissions between systems and networks, and 4) file backups. • Identifying all system components in the CDE, connected to the CDE, or that could impact security of the CDE. • Identifying all segmentation controls in use and the environment(s) from which the CDE is segmented, including justification for environments being out of scope. • Identifying all connections from third-party entities with access to the CDE. • Confirming that all identified data flows, account data, system components, segmentation controls, and connections from third parties with access to the CDE are included in scope.	*New*	x	x	Customers are responsible for documenting and maintaining PCI DSS scope, considering at minimum the factors described in this requirement.	Customers are responsible for documenting and maintaining PCI DSS scope, considering at minimum the factors described in this requirement.	Customers are responsible for documenting and maintaining PCI DSS scope, considering at minimum the factors described in this requirement.	Customers are responsible for documenting and maintaining PCI DSS scope, considering at minimum the factors described in this requirement.	Google is responsible for documenting and maintaining PCI DSS scope, considering at minimum the factors described in this requirement.
12.5.2.1 Additional requirement for service providers only: PCI DSS scope is documented and confirmed by the entity at least once every six months and upon significant change to the in-scope environment. At a minimum, the scoping validation includes all the elements specified in Requirement 12.5.2.	*New*	x	x	Customers are responsible for documenting and maintaining PCI DSS scope, considering at minimum the factors described in this requirement.	Customers are responsible for documenting and maintaining PCI DSS scope, considering at minimum the factors described in this requirement.	Customers are responsible for documenting and maintaining PCI DSS scope, considering at minimum the factors described in this requirement.	Customers are responsible for documenting and maintaining PCI DSS scope, considering at minimum the factors described in this requirement.	Google is responsible for documenting and maintaining PCI DSS scope, considering at minimum the factors described in this requirement.

PCI DSS 4.0 Requirements	PCI DSS 3.2.1	GCP	Customer	Compute	Networking	Storage	Security & Identity	Google Responsibility Summary
12.5.3 Additional requirement for service providers only: Significant changes to organizational structure result in a documented (internal) review of the impact to PCI DSS scope and applicability of controls, with results communicated to executive management.	*New*	x	x	Customers are responsible for assessing the impact of significant changes to PCI DSS scope, making appropriate updates and reporting results to executive management.	Customers are responsible for assessing the impact of significant changes to PCI DSS scope, making appropriate updates and reporting results to executive management.	Customers are responsible for assessing the impact of significant changes to PCI DSS scope, making appropriate updates and reporting results to executive management.	Customers are responsible for assessing the impact of significant changes to PCI DSS scope, making appropriate updates and reporting results to executive management.	Google is responsible for assessing the impact of significant changes to PCI DSS scope, making appropriate updates and reporting results to executive management.
12.6.1 A formal security awareness program is implemented to make all personnel aware of the entity's information security policy and procedures, and their role in protecting the cardholder data.	12.6		x	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Not Applicable
12.6.2 The security awareness program is: • Reviewed at least once every 12 months, and • Updated as needed to address any new threats and vulnerabilities that may impact the security of the entity's CDE, or the information provided to personnel about their role in protecting cardholder data.	*New*		x	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Not Applicable
12.6.3 Personnel receive security awareness training as follows: • Upon hire and at least once every 12 months. • Multiple methods of communication are used. • Personnel acknowledge at least once every 12 months that they have read and understood the information security policy and procedures.	12.6.1, 12.6.2		x	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Not Applicable
12.6.3.1 Security awareness training includes awareness of threats and vulnerabilities that could impact the security of the CDE, including but not limited to: • Phishing and related attacks. • Social engineering.	*New*		x	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Not Applicable
12.6.3.2 Security awareness training includes awareness about the acceptable use of end-user technologies in accordance with Requirement 12.2.1.	*New*		x	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Not Applicable
12.7.1 Potential personnel who will have access to the CDE are screened, within the constraints of local laws, prior to hire to minimize the risk of attacks from internal sources.	12.7		x	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Not Applicable
12.8.1 A list of all third-party service providers (TPSPs) with which account data is shared or that could affect the security of account data is maintained, including a description for each of the services provided.	12.8.1		x	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Not Applicable

PCI DSS 4.0 Requirements	PCI DSS 3.2.1	GCP	Customer	Compute	Networking	Storage	Security & Identity	Google Responsibility Summary
12.8.2 Written agreements with TPSPs are maintained as follows: • Written agreements are maintained with all TPSPs with which account data is shared or that could affect the security of the CDE. • Written agreements include acknowledgments from TPSPs that they are responsible for the security of account data the TPSPs possess or otherwise store, process, or transmit on behalf of the entity, or to the extent that they could impact the security of the entity's CDE.	12.8.2		x	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Not Applicable
12.8.3 An established process is implemented for engaging TPSPs, including proper due diligence prior to engagement.	12.8.3		x	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Not Applicable
12.8.4 A program is implemented to monitor TPSPs' PCI DSS compliance status at least once every 12 months.	12.8.4		x	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Not Applicable
12.8.5 Information is maintained about which PCI DSS requirements are managed by each TPSP, which are managed by the entity, and any that are shared between the TPSP and the entity.	12.8.5		x	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Not Applicable
12.9.1 Additional requirement for service providers only: TPSPs acknowledge in writing to customers that they are responsible for the security of account data the TPSP 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 CDE.	12.9		x	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Not Applicable
12.9.2 Additional requirement for service providers only: TPSPs support their customers' requests for information to meet Requirements 12.8.4 and 12.8.5 by providing the following upon customer request: • PCI DSS compliance status information for any service the TPSP performs on behalf of customers (Requirement 12.8.4). • Information about which PCI DSS requirements are the responsibility of the TPSP and which are the responsibility of the customer, including any shared responsibilities (Requirement 12.8.5).	*New*		x	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Not Applicable

PCI DSS 4.0 Requirements	PCI DSS 3.2.1	GCP	Customer	Compute	Networking	Storage	Security & Identity	Google Responsibility Summary
12.10.1 An incident response plan exists and is ready to be activated in the event of a suspected or confirmed security incident. The plan includes, but is not limited to: • Roles, responsibilities, and communication and contact strategies in the event of a suspected or confirmed security incident, including notification of payment brands and acquirers, at a minimum. • Incident response procedures with specific containment and mitigation activities for different types of incidents. • 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.	12.10.1		x	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Not Applicable
12.10.2 At least once every 12 months, the security incident response plan is: • Reviewed and the content is updated as needed. • Tested, including all elements listed in Requirement 12.10.1.	12.10.2		x	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Not Applicable
12.10.3 Specific personnel are designated to be available on a 24/7 basis to respond to suspected or confirmed security incidents.	12.10.3		x	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Not Applicable
12.10.4 Personnel responsible for responding to suspected and confirmed security incidents are appropriately and periodically trained on their incident response responsibilities.	12.10.4		x	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Not Applicable
12.10.4.1 The frequency of periodic training for incident response personnel is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.	*New*		x	Customers are responsible for conducting a targeted risk analysis of their control environment and determining control frequency to meet applicable PCI DSS requirements.	Customers are responsible for conducting a targeted risk analysis of their control environment and determining control frequency to meet applicable PCI DSS requirements.	Customers are responsible for conducting a targeted risk analysis of their control environment and determining control frequency to meet applicable PCI DSS requirements.	Customers are responsible for conducting a targeted risk analysis of their control environment and determining control frequency to meet applicable PCI DSS requirements.	Not Applicable
12.10.5 The security incident response plan includes monitoring and responding to alerts from security monitoring systems, including but not limited to: • Intrusion-detection and intrusion-prevention systems. • Network security controls. • Change-detection mechanisms for critical files. • The change-and tamper-detection mechanism for payment pages. This bullet is a best practice until its effective date; refer to Applicability Notes below for details. • Detection of unauthorized wireless access points.	12.10.5, 11.1.2, 11.5.1		x	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Not Applicable

PCI DSS 4.0 Requirements	PCI DSS 3.2.1	GCP	Customer	Compute	Networking	Storage	Security & Identity	Google Responsibility Summary
12.10.6 The security incident response plan is modified and evolved according to lessons learned and to incorporate industry developments.	12.10.6		x	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Not Applicable
12.10.7 Incident response procedures are in place, to be initiated upon the detection of stored PAN anywhere it is not expected, and include: • Determining what to do if PAN is discovered outside the CDE, including its retrieval, secure deletion, and/or migration into the currently defined CDE, as applicable. • Identifying whether sensitive authentication data is stored with PAN. • Determining where the account data came from and how it ended up where it was not expected. • Remediating data leaks or process gaps that resulted in the account data being where it was not expected.	*New*		x	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Customers are responsible for maintaining policies and programs that support the information security of their cardholder data environment in accordance with PCI DSS requirements.	Not Applicable
Appendix A1: Additional PCI DSS Requirements for Multi-Tenant Service Providers								
A1.1.1 Logical separation is implemented as follows: • The provider cannot access its customers' environments without authorization. • Customers cannot access the provider's environment without authorization.	*New*	x	x	Multi-tenant customers are responsible for implementing logical separation such that customer and provider environments are segmented and one environment cannot access another without authorization.	Multi-tenant customers are responsible for implementing logical separation such that customer and provider environments are segmented and one environment cannot access another without authorization.	Multi-tenant customers are responsible for implementing logical separation such that customer and provider environments are segmented and one environment cannot access another without authorization.	Multi-tenant customers are responsible for implementing logical separation such that customer and provider environments are segmented and one environment cannot access another without authorization.	Google is responsible for implementing logical separation such that customer and provider environments are segmented and one environment cannot access another without authorization.
A1.1.2 Controls are implemented such that each customer only has permission to access its own cardholder data and CDE.	A1.2	x	x	Multi-tenant customers are responsible for implementing logical separation such that each customer has access to its own cardholder data and CDE only.	Multi-tenant customers are responsible for implementing logical separation such that each customer has access to its own cardholder data and CDE only.	Multi-tenant customers are responsible for implementing logical separation such that each customer has access to its own cardholder data and CDE only.	Multi-tenant customers are responsible for implementing logical separation such that each customer has access to its own cardholder data and CDE only.	Google is responsible for implementing logical separation such that each customer has access to its own cardholder data and CDE only.
A1.1.3 Controls are implemented such that each customer can only access resources allocated to them.	A1.2	x	x	Multi-tenant customers are responsible for implementing logical separation such that customer and provider environments are segmented and one environment cannot access another without authorization.	Multi-tenant customers are responsible for implementing logical separation such that customer and provider environments are segmented and one environment cannot access another without authorization.	Multi-tenant customers are responsible for implementing logical separation such that customer and provider environments are segmented and one environment cannot access another without authorization.	Multi-tenant customers are responsible for implementing logical separation such that customer and provider environments are segmented and one environment cannot access another without authorization.	Google is responsible for implementing logical separation such that customer and provider environments are segmented and one environment cannot access another without authorization.
A1.1.4 The effectiveness of logical separation controls used to separate customer environments is confirmed at least once every six months via penetration testing.	*New*	x	x	Multi-tenant customers are responsible for conducting penetration testing to verify that customer environments are segmented in line with separation controls.	Multi-tenant customers are responsible for conducting penetration testing to verify that customer environments are segmented in line with separation controls.	Multi-tenant customers are responsible for conducting penetration testing to verify that customer environments are segmented in line with separation controls.	Multi-tenant customers are responsible for conducting penetration testing to verify that customer environments are segmented in line with separation controls.	Google is responsible for conducting penetration testing to verify that customer environments are segmented in line with separation controls.

PCI DSS 4.0 Requirements	PCI DSS 3.2.1	GCP	Customer	Compute	Networking	Storage	Security & Identity	Google Responsibility Summary
A1.2.1 Audit log capability is enabled for each customer's environment that is consistent with PCI DSS Requirement 10, including: • Logs are enabled for common third-party applications. • Logs are active by default. • Logs are available for review only by the owning customer. • Log locations are clearly communicated to the owning customer. • Log data and availability is consistent with PCI DSS Requirement 10.	A1.3	x	x	Multi-tenant customers are responsible for configuring logging parameters in alignment with PCI DSS requirements.	Multi-tenant customers are responsible for configuring logging parameters in alignment with PCI DSS requirements.	Multi-tenant customers are responsible for configuring logging parameters in alignment with PCI DSS requirements.	Multi-tenant customers are responsible for configuring logging parameters in alignment with PCI DSS requirements.	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with this requirement; failures of critical security control systems are addressed promptly.
A1.2.2 Processes or mechanisms are implemented to support and/or facilitate prompt forensic investigations in the event of a suspected or confirmed security incident for any customer.	A1.4	x	x	Multi-tenant customers are responsible for ensuring a process is implemented for timely detection and reporting of failures of critical security control systems; failures are addressed promptly.	Multi-tenant customers are responsible for ensuring a process is implemented for timely detection and reporting of failures of critical security control systems; failures are addressed promptly.	Multi-tenant customers are responsible for ensuring a process is implemented for timely detection and reporting of failures of critical security control systems; failures are addressed promptly.	Multi-tenant customers are responsible for ensuring a process is implemented for timely detection and reporting of failures of critical security control systems; failures are addressed promptly.	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with this requirement; failures of critical security control systems are addressed promptly.
A1.2.3 Processes or mechanisms are implemented for reporting and addressing suspected or confirmed security incidents and vulnerabilities, including: • Customers can securely report security incidents and vulnerabilities to the provider. • The provider addresses and remediates suspected or confirmed security incidents and vulnerabilities according to Requirement 6.3.1.	*New*	x	x	Multi-tenant customers are responsible for ensuring a process is implemented for timely detection and reporting of failures of critical security control systems; failures are addressed promptly.	Multi-tenant customers are responsible for ensuring a process is implemented for timely detection and reporting of failures of critical security control systems; failures are addressed promptly.	Multi-tenant customers are responsible for ensuring a process is implemented for timely detection and reporting of failures of critical security control systems; failures are addressed promptly.	Multi-tenant customers are responsible for ensuring a process is implemented for timely detection and reporting of failures of critical security control systems; failures are addressed promptly.	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with this requirement; failures of critical security control systems are addressed promptly.